代数学

山口大学教授
理学博士　倉田吉喜 著

現代数学
ゼミナール
16

近代科学社

現代数学ゼミナール

16

代 数 学

山口大学教授・理学博士

倉田吉喜 著

近代科学社

本書を無断で複写(コピー)することは，著作権法上認められている場合を除き，禁じられています．小社は，著者から複写(コピー)に係る権利の管理につき委託を受けていますので，複写をされる場合は，必ず小社宛ご連絡ください．

まえがき

この本は，山口大学理学部数学科における代数学の講義をもとにまとめたものである．私共の数学科では代数学の講義は3年生から始まり，4年生になって代数学特論，代数学セミナーと続く．この本は3年生の講義と，4年生のセミナーの準備を念頭において書かれた．したがって，集合論に関する基本的な事柄は既知として話をすすめている．集合論については，例えば，巻末文献の［7］等を参考にしたらよい．

第1章の群では，群の一般論に加えて置換群を手近な群の例として取り上げた．第2章の環では，整数論の基本定理が単項イデアル整域に拡張できることを示して終わりとした．初等整数論に関する注意は第1章の1.2節と1.5節に分けてのべた．その他の整数論のことはできるだけ群，環の理論の応用として示すようにした．第3章の加群では，アーベル群の基本定理をのべることを目標にしたといってもよい．3.5節では基本定理をのべ，3.6節ではその一意性を証明した．第4章の体でも話題は限られている．ガロアの理論は取り上げず，最後の節で有限体のことをやや詳しくのべた．最近の数学科にはコンピュータを勉強したいという学生が数多くいる．そういう学生のセミナーのための準備と考えてのことである．

この本で取り上げた話題は幾分限られたものになっている．しかし，群論をもう少し詳しくして，体の理論にガロアの理論を加えれば，普通の代数学の教科書とあまり変わらない内容となるはずである．むしろこの本は，私共が教室で黒板の前にたって学生に話しかけるという気持ちをこめて書かれている．したがって，分かりやすいのべ方にしているが簡潔とはとてもいえない．できるだけ分かりやすくということで数多くの例をあげ，演習問題もまた具体的なものを中心にしてある．

ふだんの講義のときもそうであるが，この本を書くにあたっても数多くの本から多くのことを学んだ．ここに記して厚く御礼申し上げたい．また同僚の大城紀代市教授には原稿を通読し，貴重な注意をのべていただいた．このことについても御礼申し上げたい．この本の執筆を始めたのがいつであったかすぐ思い出せない程長く時間がたっている．最初の頃の原稿はすっかり変色している．

この間近代科学社の方々，特に，牧野末喜氏，桜井亮志氏にはご迷惑をかけどおしであった．申し訳ないことと思っている．また，編集部の古友孝児氏には並々ならぬお世話をいただいた．深く感謝の意を表したい．

平成3年12月

倉田　吉喜

目　　次

1.　群 ……………………………………………… *1*

1.1　群の定義 ……………………………… 1
1.2　部分群 ………………………………… 10
1.3　正規部分群 …………………………… 16
1.4　群の準同型 …………………………… 24
1.5　巡回群 ………………………………… 31
1.6　置換群 ………………………………… 39
演習問題 1 ……………………………… 48

2.　環 ……………………………………………… *55*

2.1　環の定義 ……………………………… 55
2.2　イデアルと剰余環 …………………… 61
2.3　環の準同型 …………………………… 66
2.4　商　体 ………………………………… 74
2.5　多項式環 ……………………………… 79
2.6　素元分解 ……………………………… 90
演習問題 2 ……………………………… 105

3.　加　群 ………………………………………… *112*

3.1　加群と部分加群 ……………………… 112
3.2　加群の準同型 ………………………… 120
3.3　加群の直和 …………………………… 124
3.4　自由加群 ……………………………… 129
3.5　アーベル群の基本定理(1) …………… 135
3.6　アーベル群の基本定理(2) …………… 145
演習問題 3 ……………………………… 151

4.　体 ……………………………………………… *159*

4.1　拡大体 ………………………………… 159
4.2　単純拡大 ……………………………… 161
4.3　有限拡大と代数拡大 ………………… 169
4.4　分解体 ………………………………… 174
4.5　有限体 ………………………………… 179

演 習 問 題 4 …………………………………………… 188

演習問題略解……………………………………………… *193*

参 考 文 献……………………………………………… *203*

索　　引……………………………………………… *204*

記　号　表

この本では

(有理)整数の全体を　$\boldsymbol{Z}$,

有理数の全体を　$\boldsymbol{Q}$,

実数の全体を　$\boldsymbol{R}$,

複素数の全体を　$\boldsymbol{C}$,

であらわす．また，集合 S の濃度を $|S|$ であらわす．

1

群

この章でのべる群の概念は代数学で最も基本的なものの1つであり，次の章からの環，加群，体の概念はすべて群の概念を基礎にして，その上に構成されている．

1.1 群の定義

空でない集合Gに対して，GとGの直積集合

$$G\times G=\{(a,b)\mid a,b\in G\}$$

からGへの一意写像をGの上の(2項)**演算**とよぶ．

$\varphi\colon G\times G\to G$を$G$の上の演算とする．$G$がこの$\varphi$に関して

1. Gの元a,b,cに対して
$$\varphi(\varphi(a,b),c)=\varphi(a,\varphi(b,c))$$
が成り立つ，
2. あるGの元eがあって，Gの任意の元aに対して
$$\varphi(a,e)=\varphi(e,a)=a$$
が成り立つ，
3. Gの各元aに対して，あるGの元a'があって
$$\varphi(a,a')=\varphi(a',a)=e$$
が成り立つ

の3つの公理をみたすとき，Gは演算φに関して**群**をつくる，または(G,φ)は群であるという．φがはっきりしているときは，単にGは群であるともいう．

Gの上の演算φをあらわすのに，普通乗法または加法の記号を用いる．Gの元$\varphi(a,b)$を乗法の記号で$a\cdot b$または単にabであらわしたとき，(G,φ)またはGを**乗法群**，$a\cdot b$またはabをGの元aとbの**積**とよぶ．このとき，群の3つの公理は

1.　Gの元a,b,cに対して
$$(ab)c=a(bc)$$
が成り立つ，

2.　あるGの元eがあって，Gの任意の元aに対して
$$ae=ea=a$$
が成り立つ，

3.　Gの各元aに対して，あるGの元a'があって
$$aa'=a'a=e$$
が成り立つ

とかきなおされる．

これに対して加法の記号を用いて$\varphi(a,b)=a+b$とかいたとき，(G,φ)またはGを**加法群**とよび，$a+b$をGの元aとbの**和**とよぶ．このとき，公理1は

1.　Gの元a,b,cに対して
$$(a+b)+c=a+(b+c)$$
が成り立つ

とかきなおされる．公理2,3についても同様である．

これから群の一般論をのべるときは，簡単のため，Gを乗法群として扱い，単に群Gとのべることにする．

Gを群とする．Gは公理1,2,3をみたす．Gが公理1をみたすことをGは**結合法則**をみたすという．

Gには公理2をみたす元eがある．このような元はただ1個しかない．実際，Gの元e'も公理2をみたすならば，Gの任意の元aに対して$ae'=e'a=a$であり，特に，aをeにとれば，$ee'=e$が成り立つ．同じように，$ae=ea=a$でaをe'にとれば$ee'=e'$であるから，$e=ee'=e'$となる．

このただ1個存在するGの元eをGの**単位元**とよぶ．

Gの各元aに対して，公理3をみたすGの元a'が存在する．a'もまたaに依存してただ1個きまる．実際，a''も公理3をみたすならば，結合法則から
$$a'=a'e=a'(aa'')=(a'a)a''=ea''=a''$$

となる.

このaに依存してただ1個きまるa'をaの**逆元**とよび,a^{-1}であらわす. $aa^{-1}=a^{-1}a=e$であるから,aはa^{-1}の逆元の働きをしている.逆元の一意性から$a=(a^{-1})^{-1}$である.

Gが加法群のときは,Gの単位元を0とかき**零元**とよぶ.Gの元aの逆元もa^{-1}とはかかずに$-a$であらわす.Gの2元a, bに対して,数のように,$a-b$を

$$a-b=a+(-b)$$

ときめる.

例 1 0でない実数の全体を$\boldsymbol{R}^*$とかく.$\boldsymbol{R}^*$の2元a, bの積abはまた$\boldsymbol{R}^*$の元で,したがって,$\varphi(a, b)=ab$ときめて$\boldsymbol{R}^*\times\boldsymbol{R}^*$から$\boldsymbol{R}^*$への一意写像$\varphi$がきまる.この$\varphi$に関して$\boldsymbol{R}^*$は群の3つの公理をみたす.公理1は明らかである.公理2では$e=1$とおけばよく,公理3では$a'=\dfrac{1}{a}$ときめればよい.$\boldsymbol{R}^*$はこうして数の乗法を演算として群をつくる.

0でない有理数の全体$\boldsymbol{Q}^*$, 0でない複素数の全体$\boldsymbol{C}^*$も同じように数の乗法を演算として群をつくる.

例 2 2つの整数a, bの和$a+b$はまた整数であり,$\varphi(a, b)=a+b$ときめて,$\boldsymbol{Z}\times\boldsymbol{Z}$から$\boldsymbol{Z}$への一意写像$\varphi$がきまる.この$\varphi$に関して$\boldsymbol{Z}$は群をつくる.零元は数の0であり,$a'$は$-a$ときめればよい.

$\boldsymbol{Q}, \boldsymbol{R}, \boldsymbol{C}$も同じように数の加法を演算として群をつくる.

例1, 2の群では群の公理1, 2, 3のほかに次の公理

4. Gの任意の2元a, bに対して

$$ab=ba$$

が成り立つ

をみたしている.この公理を**交換法則**とよび,交換法則をもみたす群を**可換群**または**アーベル群**とよぶ.加法群では交換法則は

Gの任意の2元a, bに対して

$$a+b=b+a$$

が成り立つ

となるが,加法群とよぶときはいつもこの交換法則をみたしているものとする.

群Gの濃度 $|G|$ をGの**位数**とよび，位数有限の群を**有限群**，そうでない群を**無限群**とよぶ．例 1, 2 の群はいずれも無限群である．

空でない集合Gに演算φが与えられているとする．ここでも $\varphi(a, b)=ab$ と乗法の記号を用いることにする．Gの任意の元aに対して

$$ae=a$$

をみたすGの元eをGの**右単位元**，Gの元aに対して

$$aa'=e$$

をみたすGの元a'をaの**右逆元**とよぶ．

群の公理 2, 3 のかわりに右単位元，右逆元の概念を用いて群を定義することができる．

定理 1.1　空でない集合Gに結合法則をみたす演算が与えられているとき，この演算に関して

Gが群をつくる $\Leftrightarrow$ (1)　Gは右単位元をもつ，

(2)　Gの各元aは右逆元をもつ．

この証明は演習問題とする．Gが群をつくる条件はこれ以外にも次のようなものがある．

定理 1.2　空でない集合Gに結合法則をみたす演算が与えられているとき，この演算に関して

Gが群をつくる $\Leftrightarrow$ Gの任意の 2 元a, bに対して

$$ax=b, \quad ya=b$$

をみたすGの元x, yが存在する．

証明　$\Rightarrow$: $x=a^{-1}b$, $y=ba^{-1}$ とおけばよい．

$\Leftarrow$: G の元aをとる．仮定から

$$ae_a=a$$

をみたすGの元e_aがaに依存してきまる．Gの任意の元bに対して仮定から

$$ya=b$$

をみたすGの元yがあり，このとき

$$be_a=(ya)e_a=y(ae_a)=ya=b$$

が成り立つから，e_aはGの右単位元である．また，仮定から

$$ax=e_a$$

をみたすGの元xが存在する．xはaの右逆元であり，定理 1.1 からGは群をつくる．

Gを群，a, x, yをGの元とすると左右の**簡約律**

$$ax=ay \Rightarrow x=y, \qquad xa=ya \Rightarrow x=y$$

が成り立つ．

これは$a^{-1}(ax)=(a^{-1}a)x=ex=x$であることから明らかである．$G$が有限集合のときには，簡約律を用いて群を定義することもできる．

定理 1.3　空でない有限集合Gに結合法則をみたす演算が与えられているとき，この演算に関して

$$G\text{が群をつくる} \Leftrightarrow G\text{が左右の簡約律をみたす}.$$

証明　群Gが簡約律をみたすことは上でのべた．逆に，有限集合Gが左右の簡約律をみたすとする．Gを$\{a_1, a_2, \cdots, a_n\}$であらわす．$G$の任意の2元$a, b$に対して$aa_i$ $(1 \leqq i \leqq n)$は左簡約律により相異なるn個の元をあらわすから，全体として$a_1, a_2, \cdots, a_n$と一致する．したがって，

$$ax=b$$

をみたすGの元xが存在する．同じように，$ya=b$をみたすGの元yも存在する．定理1.2からGは群をつくる．

例 3　実数を成分とする2×2行列の全体をGとする．行列の加法は結合法則をみたすGの上の演算であり，交換法則もみたしてGは加法群をつくる．Gの零元は零行列$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$であり，$G$の元$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$の逆元は$\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$である．同じようなことは$2\times2$行列にかぎらず，一般に$m\times n$行列の全体についても成り立つ．

例 4　実数を成分とする正則な(逆行列をもった) 2×2行列の全体Gは，行列の乗法を演算として，例3と同じように，群をつくる．Gの単位元は単位行列$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$であり，$G$の元$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$の逆元は逆行列$\dfrac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$である．

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\cdot\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}=\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\cdot\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

から分かるように，Gはアーベル群ではない．

同じようなことは正則な$n\times n$行列の全体についても成り立つ．この群を$\boldsymbol{R}$の上の**一般線型群**とよび，$GL(n, \boldsymbol{R})$であらわす．$GL(n, \boldsymbol{R})$の元で行列式が1であるようなものの全体も，$GL(n, \boldsymbol{R})$と同じ演算，行列の乗法に関して群をつくる．この群を$\boldsymbol{R}$の上の**特殊線型群**とよび，$SL(n, \boldsymbol{R})$であらわす．上の例からも分かるように，この群もアーベル群とはかぎらない．

位数nの有限群Gの元を$a_1, a_2, \cdots, a_n$であらわしたとき，Gの演算を表1.1で示すことができる．

表 1.1

	a_1	a_2	$\cdots$	a_j	$\cdots$	a_n
a_1	a_1a_1	a_1a_2	$\cdots$	a_1a_j	$\cdots$	a_1a_n
a_2	a_2a_1	a_2a_2	$\cdots$	a_2a_j	$\cdots$	a_2a_n
$\vdots$	$\vdots$			$\vdots$		$\vdots$
a_i	a_ia_1		$\cdots$	a_ia_j	$\cdots$	a_ia_n
$\vdots$	$\vdots$			$\vdots$		$\vdots$
a_n	a_na_1		$\cdots$	a_na_j	$\cdots$	a_na_n

表1.1はn行n列の表で，第i行と第j列の交わる位置にa_ia_jを配置する．このような表を群Gの**乗積表**とよぶ．

群Gの乗積表を(i,j)成分がa_ia_jの$n\times n$行列とみたとき，

$$G\text{がアーベル群} \Leftrightarrow \text{この行列が対称行列}$$

は明らかである．

例 5　2つの整数1と-1の2元からなる集合Gは数の乗法を演算としてアーベル群をつくる．Gの乗積表は表1.2のようになる．

表 1.2

	1	-1
1	1	-1
-1	-1	1

このGの部分集合で1のみからなる集合HもGと同じ演算で群をつくる．Hの単位元は1，1の逆元も1である．このHのように単位元のみからなる群を特に**単位群**とよんでいる．

例 6　空でない集合Xに対して，XからXへの全単射写像をXの**置換**とよぶ．GをXの置換の全体とすると，Gの2つの元f,gを合成したfgはまたGの元で，$\varphi(f,g)=fg$ときめてGの上に演算がきまる．Gはこの演算に関して群をつくる．このことは(全単射とはかぎらず)写像の合成は常に結合法則をみたすから，定理1.1を用いても確かめることができる．Xの恒等写像がGの単位元をなし，Gの元の逆元は逆写像を考えればよい．

この群GをXの上の**対称群**という．特に，$|X|=n$のとき，GをS_nとかき**n次の対称群**とよぶ．例えば，

S_1 は X の恒等写像のみからなる単位群である．

S_2 は位数 2 のアーベル群である．この証明は演習問題とする．

S_3 では，X の元を簡単に 1, 2, 3 とかく．S_3 の元で，例えば，1 を 3 に，2 を 1 に，3 を 2 に移すものを $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ であらわす．このとき，S_3 は

$$e=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\quad a=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\quad b=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$
$$u=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\quad v=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},\quad w=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

の 6 個の元からなる．S_3 の演算は写像の合成であった．したがって，S_3 の 2 元 f, g の積 fg は，X の元 x に対して

$$(fg)(x)=f(g(x))$$

をみたす．例えば，S_3 の a, b に対しては

$$(ab)(1)=a(b(1))=a(3)=1,$$
$$(ab)(2)=a(b(2))=a(1)=2,$$
$$(ab)(3)=a(b(3))=a(2)=3$$

であるから，$ab=e$ となる．こうして S_3 の乗積表をつくると表 1.3 のようになる．この乗積表から，S_3 はアーベル群ではない．

表 1.3

	e	a	b	u	v	w
e	e	a	b	u	v	w
a	a	b	e	w	u	v
b	b	e	a	v	w	u
u	u	v	w	e	a	b
v	v	w	u	b	e	a
w	w	u	v	a	b	e

例 7　平面 α の置換の全体 G も，写像の合成を演算として群をつくる．α の 2 点 P, Q の距離を $\overline{\mathrm{PQ}}$ とかく．G の元 f で α の任意の 2 点 P, Q に対して

$$\overline{f(\mathrm{P})f(\mathrm{Q})}=\overline{\mathrm{PQ}}$$

をみたすものを，特に，α の**運動**とよぶ．α の運動の全体を H とかく．H は G の部分集合である．

$f, g \in H$ とする．f に対して，特に，$\overline{f(g(\mathrm{P}))f(g(\mathrm{Q}))}=\overline{g(\mathrm{P})g(\mathrm{Q})}$ が成り立つから

$$\overline{(fg)(\mathrm{P})(fg)(\mathrm{Q})}=\overline{f(g(\mathrm{P}))f(g(\mathrm{Q}))}=\overline{g(\mathrm{P})g(\mathrm{Q})}=\overline{\mathrm{PQ}}$$

であって，f, g の合成 fg がまた α の運動であることが分かる．すなわち，

$$f, g\in H \Rightarrow fg\in H. \qquad (1)$$

このことは，G の演算 $\varphi: G\times G\to G$ を $H\times H$ に制限すると φ が

$$\varphi: H\times H\to H$$

なる写像であることを示している．

α の恒等写像 1_α は明らかに α の運動である．すなわち，

$$1_\alpha\in H. \qquad (2)$$

$f\in H$ とする．f は α の置換であるから f^{-1} が存在して，$\overline{f(f^{-1}(\mathrm{P}))f(f^{-1}(\mathrm{Q}))}=\overline{f^{-1}(\mathrm{P})f^{-1}(\mathrm{Q})}$ であるから

$$\overline{\mathrm{PQ}}=\overline{(ff^{-1})(\mathrm{P})(ff^{-1})(\mathrm{Q})}=\overline{f(f^{-1}(\mathrm{P}))f(f^{-1}(\mathrm{Q}))}=\overline{f^{-1}(\mathrm{P})f^{-1}(\mathrm{Q})}$$

が成り立って，f^{-1} もまた α の運動であることが分かる．すなわち，

$$f\in H \Rightarrow f^{-1}\in H. \qquad (3)$$

以上のことから，α の運動の全体 H は α の置換の全体 G の部分集合であり，H 自身 G と同じ演算で群をつくっていることが分かる．

例 8　上の例と同じように，平面 α の置換の全体を G, α の運動の全体を H とする．α の上に正三角形 ABC を考える．H の元で正三角形 ABC をそれ自身に重ねるようなものの全体も，H と同じ，したがって G と同じ演算で群をつくる．この群を D_3 とかき，3 次の**二面体群**とよぶ．

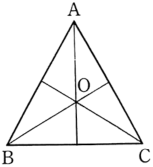


図 1.1

正三角形の重心 O を通って α に垂直な直線を回転軸として，正の向きに 0°, 120°, 240° の回転をそれぞれ e, a, b とかき，直線 AO, BO, CO に関する対称運動をそれぞれ u, v, w とかけば，D_3 はこの 6 個の元 e, a, b, u, v, w からなる群である．

実際，頂点 A, B, C を簡単に 1, 2, 3 とかきなおすと，D_3 の元は $X=\{1, 2, 3\}$ の置換をひきおこす．例えば，$a=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$ であり，$u=\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$ である．逆

に，Xの置換は正三角形 ABC をそれ自身に重ねるαの運動で，したがって，D_3は例 6 のS_3に一致する．

この節の最後に，群の一般論にもどって基本性質をいくつかのべる．

(1)　Gを群，$a_1, a_2, \cdots, a_n$ $(n \geqq 3)$ をGの元とする．このn個の元の積$a_1 a_2 \cdots a_n$を帰納的に

$$a_1 a_2 \cdots a_n = (a_1 a_2 \cdots a_{n-1}) \cdot a_n$$

ときめる．$n=3$のときは，

$$a_1 a_2 a_3 = (a_1 a_2) a_3$$

であり，これは結合法則によって$a_1(a_2 a_3)$とも一致する．$n=4$ならば，

$$a_1 a_2 a_3 a_4 = (a_1 a_2 a_3) a_4$$

であるが，結合法則によって$((a_1 a_2) a_3) a_4$, $(a_1 a_2)(a_3 a_4)$, $a_1(a_2(a_3 a_4))$等と一致する．このようにGの元の 4 個の積もどのようにかっこでくくってもすべて一致する．このことは一般にn個の元の積のときにも成り立ち，帰納法によって証明できるがここでは省略する．

(2)　Gを群，$a_1, a_2, \cdots, a_n$をGの元とする．

$$(a_1 a_2) \cdot (a_2^{-1} a_1^{-1}) = a_1 (a_2 a_2^{-1}) a_1^{-1} = a_1 a_1^{-1} = e$$

であり，$(a_2^{-1} a_1^{-1}) \cdot (a_1 a_2)$も同じように$e$に等しい．したがって，$(a_1 a_2)^{-1} = a_2^{-1} a_1^{-1}$であり，一般に

$$(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1}$$

が成り立つ．

(3)　Gを群，aをGの元とする．任意の自然数nに対して，(1) よりn個のaの積a^nがきまる．その上，

$$a^0 = e, \quad a^{-n} = (a^n)^{-1} = (a^{-1})^n$$

ときめると，次の**指数法則**が成り立つ．

定理 1.4　Gを群，a, bをGの元とする．任意の整数m, nに対して

$$a^m a^n = a^{m+n}, \qquad (a^m)^n = a^{mn}$$

が成り立つ．特にa, bが$ab = ba$をみたすときは，任意の整数mに対して

$$(ab)^m = a^m b^m$$

である．

証明　$a^m a^n = a^{m+n}$の証明のみ簡単にのべる．m, nの正，負，0により場合を分ける．$m=0$か$n=0$のときは明らかであるから，$m>0$で$n>0$のとき，$m>0$で$n<0$のとき，$m<0$で$n>0$のとき，$m<0$で$n<0$のときの 4 つの場

合を考える．$m>0, n>0$ の場合は $a^m a^n$ も a^{m+n} も共に $(m+n)$ 個の a の積であるから，この2つは一致する．$m>0, n<0$ ときは $n=-n', n'>0$ とおけば，

$$a^m a^n = a^m (a^{-1})^{n'} = \begin{cases} a^{m-n'} & (m \geqq n' \text{ のとき}) \\ (a^{-1})^{n'-m} & (m<n' \text{ のとき}) \end{cases}.$$

ここで $(a^{-1})^{n'-m} = a^{-(n'-m)} = a^{m-n'}$ であるから，いずれの場合も

$$a^m a^n = a^{m-n'} = a^{m+n}$$

が成り立つ．残りの場合も同じように証明できる．

Gが加法群のときは，乗法のところを加法にかきなおして，整数 m とGの元 a に対して ma は

$$ma = \begin{cases} a \text{ の } m \text{ 個の和} & (m>0 \text{ のとき}), \\ 0 & (m=0 \text{ のとき}), \\ a \text{ の } |m| \text{ 個の和の逆元} & (m<0 \text{ のとき}) \end{cases}$$

を意味する．ここで $|m|$ はmの絶対値をあらわす．$m<0$ のときは

$$ma = (-a) \text{ の } |m| \text{ 個の和}$$

とのべてもよい．

加法群Gでは，指数法則はGの元 a, b，整数 m, n に対して

$$ma+na=(m+n)a, \quad m(na)=(mn)a,$$
$$m(a+b)=ma+mb$$

とあらわされる．

1.2 部　分　群

(G, φ) を群とする．1.1節にならって，$\varphi(a, b)=ab$ とかく．HがGの空でない部分集合で

(1) $a, b \in H \Rightarrow a$ と b のGにおける積 $ab \in H$,

(2) Gの単位元 $e \in H$,

(3) $a \in H \Rightarrow G$ における a の逆元 $a^{-1} \in H$

の3つの条件をみたすとき，HをGの φ に関する（または (G, φ) の）**部分群**とよぶ．φ がはっきりしているときは，簡単に，Gの部分群ともよぶ．

このとき，1.1節例7でも示したように，Gの演算 $\varphi: G \times G \to G$ を $H \times H$ に制限すれば，(1) から，φ は

$$\varphi: H \times H \to H$$

なる一意写像とみることができる．すなわち，Gの演算φがそのままHの演算になっている．

(2) から，Gの単位元eがHに属する．Hの任意の元aに対して，aはGの元でもあるから

$$ae=ea=a$$

が成り立つ．このことはeがHの単位元であることを示している．

(3) からは，Hの元aに対して，Gにおけるaの逆元a^{-1}がHに属する．aはGの元でもあるから

$$a\cdot a^{-1}=a^{-1}\cdot a=e$$

が成り立つ．このことはa^{-1}がHにおけるaの逆元でもあることを示している．

Gが結合法則をみたすから，もちろん，Hも結合法則をみたす．

したがって，群の定義にもどって，または定理1.1によって，H自身がGの演算に関して群をつくっている．逆に，群Gの部分集合HがGの演算に関して群をつくるならば，(1), (2), (3) が成り立ってHはGの部分群となる．この証明は演習問題とする．このことから，群Gの部分群とはGの演算に関して群をつくるGの部分集合にほかならない．

G自身Gの部分群であり，Gの単位元eのみからなる部分集合$\{e\}$もGの部分群で，この2つをGの**自明な部分群**とよぶ．

例 1 1.1節例7で示したように，平面αの運動の全体Hはαの上の対称群Gの部分群である．

例 2 $\boldsymbol{Q}$は数の加法を演算として群をつくる．$\boldsymbol{Z}$は$\boldsymbol{Q}$の空でない部分集合であり，1.1節例2で示したように，$\boldsymbol{Q}$と同じ数の加法を演算として群をつくるから，加法群$\boldsymbol{Q}$の部分群である．

加法群$\boldsymbol{Q}$はまた加法群$\boldsymbol{R}$の部分群である．したがって，$\boldsymbol{Z}$は加法群$\boldsymbol{R}$の部分群でもある．一般に，Hが群Gの部分群であり，KがHの部分群ならば，KはGの部分群でもある．この証明は演習問題とする．

同じようなことは乗法群$\boldsymbol{Q}^*, \boldsymbol{R}^*, \boldsymbol{C}^*$ (1.1節例1) についても成り立つ．$\boldsymbol{R}^*$は$\boldsymbol{R}$の部分集合であり，乗法を演算として群をつくっているが，加法群$\boldsymbol{R}$の部分群ではない．

定理 1.5 Gが群，HがGの部分集合とする．このとき，

$$H\text{が}G\text{の部分群} \Leftrightarrow \begin{array}{ll}(1)+(3) & a, b\in H \Rightarrow ab^{-1}\in H, \\ (2) & G\text{の単位元 } e\in H.\end{array}$$

証明 (1)+(3) は部分群の条件 (1) と (3) をあわせた条件をあらわす．HがG

の部分群ならば，(2) は明らかである．$a, b \in H$ ならば，b の G における逆元 $b^{-1} \in H$ であり，したがって，a, b^{-1} の G における積 $ab^{-1} \in H$ である．

逆に，(1)+(3) と (2) を仮定する．(2) から $e \in H$ であるから，(1)+(3) で a として e がとれる．このとき，(1)+(3) から $b \in H$ ならば $b^{-1} \in H$ が分かる．

$a, b \in H$ ならば，$b^{-1} \in H$ であり，(1)+(3) から $a \cdot (b^{-1})^{-1} \in H$ であるが，これは $ab \in H$ を意味する．したがって，H は G の部分群である．

定理 1.5 の (2) は $H \neq \phi$ なる条件でおきかえてもよい．すなわち，

$$H \text{が} G \text{の部分群} \Leftrightarrow \begin{array}{ll} (1)+(3) & a, b \in H \Rightarrow ab^{-1} \in H, \\ (2)' & H \neq \phi. \end{array}$$

実際，H が G の部分群ならば，H は G の単位元 e を含むから $H \neq \phi$.

逆に，$H \neq \phi$ ならば，H はある元 a を含む．(1)+(3) で $a=b$ とみれば，$H \ni aa^{-1}=e$ となり定理 1.5 の (2) をうる．

例 3　乗法群 $\boldsymbol{C}^*$ の部分集合

$$T=\{z \in \boldsymbol{C}^* \mid |z|=1\}$$

は $\boldsymbol{C}^*$ の部分群である．ここで $|z|$ は z の絶対値をあらわす．この T を 1 次元の**トーラス群**とよぶ．

実際，$|1|=1$ であり，$|z|=|z'|=1$ ならば $\left|\dfrac{z'}{z}\right|=\dfrac{|z'|}{|z|}=1$ であるから，$\dfrac{z'}{z} \in T$ で定理 1.5 から T は $\boldsymbol{C}^*$ の部分群である．

例 4　1.1 節例 4 の $SL(n, \boldsymbol{R})$ は $GL(n, \boldsymbol{R})$ の部分群である．

例 5　1.1 節例 8 の 3 次の二面体群 D_3 は，平面 α 上の運動の全体 H の部分群であり，また，α の置換の全体 G の部分群でもある．

H が有限部分集合のときはもっと簡単で，次の定理が成り立つ．

定理 1.6　G が群，H が G の空でない有限部分集合ならば，

$$H \text{が} G \text{の部分群} \Leftrightarrow (a, b \in H \Rightarrow ab \in H).$$

証明　$a, b \in H$ ならば $ab \in H$ を仮定する．すぐ上に注意したように，$a, b \in H$ ならば $ab^{-1} \in H$ を示せばよい．

b が G の単位元 e のときは明らかであるから $b \neq e$ とする．仮定から $b, b^2, b^3, \cdots$ はすべて H に属するが，H は有限集合であるから，ある自然数 m, n があって $b^m=b^n$ でなければならない．$m>n$ とする．このとき，$b^{m-n}=e$ であるが $b \neq e$ であるから $m-n \neq 1$，$m-n-1>0$ である．その上，

$$b \cdot b^{m-n-1}=b^{m-n-1} \cdot b=b^{m-n}=e$$

であるから，$b^{m-n-1}=b^{-1}$．b のべきはすべてHに属するから $b^{-1}\in H$ となり，したがって，仮定から $ab^{-1}\in H$ をうる．

例 6 定理 1.6 から 1.1 節例 5 の $G=\{1,-1\}$ は乗法群 $\boldsymbol{Q}^*$ の部分群である．

次の例は基本的である．

例 7 群Gの空でない部分集合Sに対して，$S^{-1}=\{x^{-1}\mid x\in S\}$ とおく．

S または S^{-1} に属する有限個の元の積の全体

を (S) とかく．ここで 1 個の元も積と考える．このとき，

(1) (S) はSを含むGの最小の部分群である．

この意味で (S) をSから**生成**されたGの部分群，Sを (S) の**生成系**とよぶ．

(2) $(S)=\cap\{H\mid H$ はSを含むGの部分群$\}$．

実際，(S) は S を含み，したがって，$(S)\neq\phi$．(S) の 2 元 $a=x_1x_2\cdots x_m$, $b=y_1y_2\cdots y_n$ をとる．ここで各 x_i, y_j はS または S^{-1} に属する．

$$ab^{-1}=x_1x_2\cdots x_m y_n{}^{-1}y_{n-1}{}^{-1}\cdots y_1{}^{-1}$$

で，x_i も $y_j{}^{-1}$ も S または S^{-1} に属するから ab^{-1} は (S) に属する．定理 1.5 から (S) はGの部分群である．

次に，Sを含むGの任意の部分群をHとして $(S)\subseteqq H$ を示す．(S) の任意の元 $a=x_1x_2\cdots x_m$ で各 x_i はS または S^{-1} に属するからHに属し，したがって，積 a もHに属する．

(2) は (1) から明らか．いくつかの部分群の共通部分はまた部分群であることに注意したらよい．

特に，SがGの元xのみからなるときは，$S^{-1}=\{x^{-1}\}$ であり，したがって，

$$(S)=\{x^m\mid m\in\boldsymbol{Z}\}$$

となる．これを簡単に (x) とかき，xから生成されたGの**巡回部分群**，xを (x) の**生成元**とよぶ．

例 8 乗法群 $\boldsymbol{R}^*$ で，-1 から生成された巡回部分群 (-1) は

$$\{(-1)^m\mid m\in\boldsymbol{Z}\}=\{1,-1\}$$

で，1.1 節例 5 のGと一致する．

乗法群 $\boldsymbol{C}^*$ で虚数単位 i から生成された巡回部分群 (i) は

$$\{i^m\mid m\in\boldsymbol{Z}\}=\{1,i,-1,-i\}$$

で，1 の 4 乗根の全体にほかならない．

例 9 加法群 $\boldsymbol{Z}$ では，整数xから生成された巡回部分群 (x) は（加法群であるから x^m ではなくて）

$$\{mx\mid m\in\boldsymbol{Z}\}$$

で，x の倍数の全体に等しい．明らかに，$(x)=(-x)$ でもある．

2つの整数 x, y に対して，$S=\{x, y\}$ から生成された $\boldsymbol{Z}$ の部分群は，x, y または $-x, -y$ の有限個の（積ではなくて）和の全体であるから，x の項と y の項とに分けて

$$(S)=\{mx+ny \mid m, n\in\boldsymbol{Z}\}.$$

2個以上の整数に対しても同じようなことが成り立つ．

これからしばしば例として $\boldsymbol{Z}$ をとりあげるので，ここで整数について二，三の注意をのべる．

(1)　自然数からなる空でない集合は最小数をもつ．

証明　自然数からなる空でない集合で最小数をもたないものがあったと仮定する．この集合を S とし，自然数 n に関する命題

(A)　n より小さな自然数は S に属さない

を考え，n に関する帰納法で矛盾をみちびく．1より小さな自然数はありえないから，$n=1$ は (A) をみたす．n が (A) をみたし，$n\in S$ ならば，S は最小数 n をもって仮定に反する．したがって，n が (A) をみたせば，n は S に属さない．このことは $n+1$ も (A) をみたすことを意味する．すべての自然数 n が (A) をみたし，いかなる自然数も S に属さない．これは S が空でないことに矛盾する．

(2)　S が整数からなる空でない集合で，ある整数 a があって

(B)　S の任意の元 x に対して $a\leqq x$

をみたすならば，S は最小数をもつ．

条件 (B) をみたす a を S の**下界**という．S の下界はかならずしも S の元とはかぎらない．a が S の下界ならば，a より小さな整数も S の下界である．

証明　S が自然数のみからなるときは，(1) から S はいつでも最小数をもつ．S が0または負の整数を含むものとする．a が S の下界ならば，S の任意の元 x に対して $a-1<x$ であるから，S は S のすべての元より小さな下界をもつ．このような下界すべての集合は負の整数のみからなる空でない集合で，(1) から最大数 m をもつ．S の任意の元 x に対して $m<x$ であり，したがって，$m+1\leqq x$ である．しかし，m の最大性から，S の任意の元 x に対して $m+1<x$ とはなりえず，ある $x_0\in S$ があって $m+1=x_0$ が成り立つ．このことは x_0 が S の最小数であることを示している．

条件 (B) の不等式の向きをかえて S の上界が定義できる．S が上界をもてば S は最大数をもつことも同じようにして示すことができる．

(3) a, b は整数で $b>0$ のとき,

$$nb \leqq a < (n+1)b$$

をみたす整数 n が存在する.

証明 $$S=\{nb \mid nb>a, n\in \boldsymbol{Z}\}$$

とおく. S は空でない整数の集合で a は S の下界であるから, (2) から最小数をもつ. それを $(n+1)b$ とかく. $(n+1)b$ は S の元であるから $(n+1)b>a$ であるが, もし $nb>a$ ならば $nb\in S, nb\geqq(n+1)b$. これから $0\geqq b$ となって矛盾である. したがって, $nb\leqq a$.

(4) **(除法の定理)** a, b が整数で $b\neq 0$ ならば,

$$a=bq+r \qquad (0\leqq r<|b|)$$

をみたす整数 q, r が a, b に対して一意的にきまる. ここで $|b|$ は b の絶対値をあらわす.

証明 $|b|>0$ から (3) より

$$q\cdot|b|\leqq a<(q+1)\cdot|b|$$

をみたす整数 q がある. $r=a-|b|\cdot q$ とおけば $a=|b|\cdot q+r$ $(0\leqq r<|b|)$ となる. $b>0$ のときは $a=bq+r$ であり, $b<0$ のときは $a=b(-q)+r$ である.

一意性を示すために,

$$a=bq_1+r_1=bq_2+r_2 \qquad (0\leqq r_1, r_2<|b|)$$

とおく. $|b|\cdot|q_1-q_2|=|r_2-r_1|$ で, $q_1\neq q_2$ ならば左辺は $|b|\cdot|q_1-q_2|\geqq|b|$ であり, 右辺は $|r_2-r_1|\leqq|r_2|<|b|$ で矛盾である. したがって, $q_1=q_2$ であり, かつ $r_1=r_2$ である.

除法の定理から a, b に対してただ一通りにきまる q, r をそれぞれ a を b で割ったときの**商**, **剰余**とよぶ.

特に, $r=0$ のとき, $a=bq$ となり, a は b で割り切れる. これを

$$b|a$$

とあらわし, b を a の**約数**, a を b の**倍数**とよぶ.

1より大きな自然数 p が, 自然数 a に対して

$$a|p \Rightarrow a=1 \text{ かまたは } a=p$$

をみたすとき, p を**素数**とよぶ. 2, 3, 5, 7, 11, ⋯ 等は素数である. 1より大きな自然数で素数でないものを**合成数**とよぶ.

例 10 自然数 m から生成された加法群 $\boldsymbol{Z}$ の巡回部分群 (m) は, m の倍数の全体である (例 9). (m) を $\boldsymbol{Z}m$ ともかく. 逆に,

加法群 $\boldsymbol{Z}$ の $\{0\}$ でない部分群は，適当な自然数 m から生成された巡回部分群 (m) である

ことを示す．H を $\{0\}$ でない $\boldsymbol{Z}$ の部分群とする．H は 0 でない整数 n を含む．H は n と共に $-n$ も含むから，H が自然数を含んでいるとしてよい．H に含まれる自然数の中に最小数がある．それを m とする．このとき $H=(m)$ が成り立つ．

$m\in H$ であり，(m) は m を含む $\boldsymbol{Z}$ の最小の部分群であるから $(m)\subseteqq H$．逆に，H の任意の元 a をとり，m で割って

$$a=mq+r \qquad (0\leqq r<m)$$

とおく．$r=a-mq\in H$ であるが，$r>0$ ならば $0<r<m$ となって m の最小性に矛盾するから $r=0$ でなければならない．$a=mq\in(m)$ となり，$H\subseteqq(m)$ である．

1.3　正規部分群

G を群，H を G の部分群とする．G の 2 元 a, b は $a^{-1}b\in H$ であるとき，H を法として**左合同**であるといい，

$$a\equiv b \pmod{H}$$

とかく．このとき，$\equiv$ は G の上の同値関係である．すなわち，$a, b, c\in G$ に対して

(1)　反射律　$a\equiv a \pmod{H}$,

(2)　対称律　$a\equiv b \pmod{H} \Rightarrow b\equiv a \pmod{H}$,

(3)　推移律　$a\equiv b \pmod{H}$，$b\equiv c \pmod{H} \Rightarrow a\equiv c \pmod{H}$

が成り立つ．

(1) は $a^{-1}a=e\in H$, (2) は $a^{-1}b\in H$ ならば $b^{-1}a=(a^{-1}b)^{-1}\in H$, (3) は $a^{-1}b\in H$, $b^{-1}c\in H$ ならば $a^{-1}c=a^{-1}b\cdot b^{-1}c\in H$ から，明らかである．

この同値関係によって a と同値な G の元の全体を $C(a)$ とかく．

$$C(a)=\{b\in G \mid a\equiv b \pmod{H}\}=\{b\in G \mid a^{-1}b\in H\}.$$

$C(a)$ を H を法とする a の**左剰余類**とよぶ．$C(a)$ に関しては次のことが成り立つ．

補題 1.7　(1)　$a\in C(a)$,

(2)　$C(a)=C(b) \Leftrightarrow C(a)\cap C(b)\neq\phi \Leftrightarrow a\equiv b \pmod{H}$,

(3)　$G=\bigcup\,\{C(a) \mid a\in G\}$.

証明 (1)は明らか，(3)は(1)からえられるから(2)のみ示す．

$C(a)=C(b)$ ならば，$C(a)\cap C(b)=C(a)\neq\phi$ である．次に，$C(a)\cap C(b)\neq\phi$ として $c\in C(a)\cap C(b)$ ならば，$c\equiv a \pmod{H}, c\equiv b \pmod{H}$，したがって，$a\equiv b \pmod{H}$ が分かる．逆に，$a\equiv b \pmod{H}$ ならば，b と同値なものは a とも同値であるから $C(b)\subseteqq C(a)$ である．同じようにして，$C(a)\subseteqq C(b)$ でもある．

Hを法とする左剰余類の全体 $\{C(a)\mid a\in G\}$ の中から異なったもののみを拾いあげて，その全体を

$$\{C(a)\mid a\in G'\}$$

とかく．このとき

(1) G' のどの2元もHを法として左合同ではありえない．

(2) 任意のGの元はいずれかのG'の元とHを法として左合同である．

すなわち，

$$G=\cup\{C(a)\mid a\in G'\}$$

でGは互いに共通な元をもたず，かつ空でないいくつかの左剰余類に分割される．このような分割をGの**類別**ともよぶ．

この分割では，1つの左剰余類 $C(a)$ に属する任意の元 b は他の左剰余類に属することはありえないから，$C(a)$ は b の属する左剰余類という意味で，b が $C(a)$ を代表しているとみることができる．b を $C(a)$ の**代表元**とよぶ．

b は $C(a)$ の任意の元でよかったから，$C(a)$ のどの元も $C(a)$ の代表元である．a を G' の中をわたらせて，各 $C(a)$ の中から1つずつ元をとりだしてつくった集合は，いわば各 $C(a)$ の代表元の集まりなわけで，これを G の H を法とする**完全代表系**とよぶ．G' は完全代表系の1つである．

例 1 加法群 $\boldsymbol{Z}$ の部分群 (2) は2の倍数の全体からなる部分群である．$\boldsymbol{Z}$ の2元 a, b が (2) を法として左合同とは（群の演算が加法であるから）

$$-a+b\in(2), \text{ いいかえれば, } 2|a-b$$

を意味する．このとき，

$$2|a \Leftrightarrow 2|b$$

で，$2|a-b$ は2で割って a, b が同じ剰余をもつことを意味する．したがって，(2) を法とする a の左剰余類は

$$C(a)=\{b\in\boldsymbol{Z}\mid b \text{ は2で割って } a \text{ と剰余が同じ}\}.$$

2で割ったときの剰余は0と1の2つしかないから，相異なる左剰余類は

$$C(0)=(2) \quad と \quad C(1)$$

の2つしかない．この2つの左剰余類から1個ずつ元をとりだしてつくった集合，例えば，$\{0,1\}$，$\{2,3\}$，$\{-4,-5\}$，$\cdots$ 等が $\boldsymbol{Z}$ の (2) を法とする完全代表系をつくる．

最初の一般論にもどって，群 G の部分群 H を法とする左剰余類の具体的な形をきめるため，次のように G の部分集合の積を考える．

群 G の部分集合 S, S' の積 SS' を

$$SS'=\{ss' \mid s\in S, s'\in S'\}$$

ときめる．G の3つの部分集合 S, S', S'' に対して群の公理1から

$$(SS')S''=S(S'S'')$$

が成り立つ．

特に，S が1元 s のみからなる集合のとき，積 $\{s\}S'$ を簡単に sS' とかく．すなわち，

$$sS'=\{ss' \mid s'\in S'\}.$$

S' が1元 s' のみからなるときも同じように

$$S\{s'\}=Ss'=\{ss' \mid s\in S\}$$

とする．

a の左剰余類は $C(a)=\{b\in G \mid a^{-1}b\in H\}$ であるが，

$$a^{-1}b\in H \Leftrightarrow ある\ h\in H があって\ a^{-1}b=h$$
$$\Leftrightarrow ある\ h\in H があって\ b=ah.$$

したがって，$b\in C(a)$ は $b\in aH$ を意味し

$$C(a)=aH=\{ah \mid h\in H\}$$

とあらわされる．

$a\in H$ ならば，$aH\subseteqq H$ は明らかであるが，$a^{-1}\in H$ でもあるから H の元 h を

$$h=a(a^{-1}h)$$

とかけば，$h\in aH$ が分かる．したがって，$aH=H$ が成り立つ．

逆に，$aH=H$ ならば $a=ae\in aH$ で，$a\in H$ をうる．すなわち，

$$a\in H \Leftrightarrow aH=H.$$

特に，G の単位元 e に対しては

$$eH=H.$$

H を法とする左合同と同じように，H を法とする右合同が考えられる．G の2元 a, b に対して，$ab^{-1}\in H$ であるとき，a, b は H を法として**右合同**であると

いう．このとき，Hを法とするaの右剰余類はHaで与えられる．

Hを法とする左剰余類の全体の集合から右剰余類の全体の集合への写像

$$aH \to Ha^{-1}$$

を考える．$b \in aH \Leftrightarrow b^{-1} \in Ha^{-1}$ であるから

$$aH = bH \Leftrightarrow Ha^{-1} = Hb^{-1}.$$

したがって，この写像は一意写像であり，かつ全単射である．

定理 1.8 Gを群，HをGの部分群とする．Hを法とする相異なる左剰余類の個数と，Hを法とする相異なる右剰余類の個数とは一致する．

この一致した個数をGにおけるHの**指数**といい，$(G:H)$ であらわす．

Hが自明な部分群の場合の指数は

$$H = G \Leftrightarrow (G:H) = 1,$$

$$H = \{e\} \Leftrightarrow (G:H) = |G|$$

で与えられる．実際，$H = G$ のときは

$$H = G \Leftrightarrow G \text{ の任意の元 } a \text{ に対して } aH = H$$

$$\Leftrightarrow H \text{ を法とする左剰余類は } H \text{ のみ}$$

であり，また，$H = \{e\}$ のときは

$$H = \{e\} \Leftrightarrow G \text{ の任意の元 } a \text{ に対して } aH = \{a\}.$$

これは各左剰余類が1元のみからなることを示しているから

$$\Leftrightarrow (G:H) = |G|.$$

例 2 mを自然数として加法群$\boldsymbol{Z}$の部分群(m)を法とする左合同を考える．加法群はアーベル群であって左合同，右合同，左剰余類，右剰余類を区別する必要がないから，以下単に合同，剰余類とよぶことにする．

(m)を法とする合同も簡単にmを法とする合同とよび，$\boldsymbol{Z}$の元a, bがmを法として合同のとき $a \equiv b \pmod{m}$ とかく．

mを法とするaの剰余類は(演算が加法であるから)

$$C(a) = a + (m) = \{a + mc \mid c \in \boldsymbol{Z}\}$$

であらわされる．

$a = mq + r$ $(0 \leqq r < m)$ とかけば

$$a + mc = m(q + c) + r$$

であるから，$a + mc$ はmで割ってaと同じ剰余をもつ整数を意味する．

$$C(a) = \{b \in \boldsymbol{Z} \mid b \text{ は } m \text{ で割って } a \text{ と同じ剰余}\}.$$

したがって，mを法とする剰余類の全体 $\{C(a) \mid a \in \boldsymbol{Z}\}$ の中から異なるものを拾いだすには，mで割って異なる剰余をもつものを集めればよく，異なった剰

余は $0, 1, 2, \cdots, m-1$ であるから

$$C(0), C(1), \cdots, C(m-1)$$

が異なる剰余類の全体をつくす．このことから

$$(\boldsymbol{Z}:(m))=m$$

が分かる．したがって，

$$0, 1, 2, \cdots, m-1$$

は $\boldsymbol{Z}$ の m を法とする完全代表系であり，$m\in C(0), m+1\in C(1), \cdots, 2m-1\in C(m-1)$ であるから

$$m, m+1, \cdots, 2m-1$$

もまた完全代表系である．

例 3　1.1 節例 6 の S_3 で，a から生成された巡回部分群 (a) は

$$a^2=b,\quad a^3=aa^2=ab=e,\quad a^4=a,\quad a^5=a^2, \cdots$$

であるから

$$(a)=\{a^n \mid n\in\boldsymbol{Z}\}=\{e, a, a^2\}=\{e, a, b\}$$

であり，u から生成された巡回部分群 (u) は

$$u^2=e,\quad u^3=uu^2=u,\quad u^4=e, \cdots$$

であるから

$$(u)=\{u^n \mid n\in\boldsymbol{Z}\}=\{e, u\}$$

である．(a) を法とする u の左剰余類，右剰余類は

$$u(a)=\{ue, ua, ub\}=\{u, v, w\},$$
$$(a)u=\{eu, au, bu\}=\{u, w, v\}$$

と両者は一致する．しかし，(u) を法とする v の左剰余類，右剰余類は

$$v(u)=\{v, b\},\quad (u)v=\{v, a\}$$

で両者は異なる．

Gを群，HをGの部分群とする．Gの元 a に対して，写像

$$H\to aH,\quad h\to ah$$

は明らかに一意写像，かつ全単射である．したがって，

補題 1.9　Gが群，HがGの部分群ならば，Hを法とする左（右）剰余類はすべてHの位数と同じ濃度をもつ．

定理 1.10　Gが有限群，HがGの部分群ならば

$$|G|=(G:H)\cdot|H|.$$

系 1.11（ラグランジュ）　有限群Gの部分群の位数はGの位数の約数である．

Gを群，HをGの部分群とする．例3にのべたように，Hを法とするaの左剰余類aHと右剰余類Haとは一致することもあり，そうでないこともある．特に，Gのすべての元aに対して

$$aH=Ha$$

が成り立つとき，HをGの**正規部分群**とよび，$H\lhd G$であらわす．このとき左剰余類，右剰余類を区別せず単に剰余類とよんでよい．

Gがアーベル群ならばGの部分群はすべて正規部分群であるが，Gがアーベル群でなくても自明な部分群はいつも正規部分群である．Gの元aに対して，$a\{e\}=\{e\}a=\{a\}$であり，$aG=Ga=G$である．

群Gの正規部分群が自明な部分群しかないとき，Gを**単純群**とよぶ．

定理 1.12 群Gの部分群Hに対して，次は同値である．

(1) HはGの正規部分群である．

(2) 任意のGの元aに対して$aH\subseteqq Ha$が成り立つ．

(3) 任意のGの元aに対して$aHa^{-1}\subseteqq H$が成り立つ．

証明 (1) ⇒ (2) ⇒ (3) は明らか．(3) ⇒ (1) を示す．任意のGの元aに対して$aHa^{-1}\subseteqq H$を仮定する．Hの元hに対して$ah=(aha^{-1})a\in Ha$であるから，$aH\subseteqq Ha$をうる．仮定から$a^{-1}H(a^{-1})^{-1}\subseteqq H$でもあり，したがって，$a^{-1}Ha\subseteqq H$. 同じようにして$Ha\subseteqq aH$となり，$aH=Ha$である．

例 4 1.1節例4の$SL(n,\boldsymbol{R})$は$GL(n,\boldsymbol{R})$の部分群であるが，実は正規部分群である．

このことは，実数を成分とする正則な$n\times n$行列Aと，任意の$n\times n$行列Bとに対して$|ABA^{-1}|=|A|\cdot|B|\cdot|A^{-1}|=|A|\cdot|A^{-1}|\cdot|B|=|B|$であることから，明らか．ここで$|A|$は行列$A$の行列式をあらわす．

例 5 指数2の部分群は正規部分群である．

Gを群，Hを指数2の部分群とする．Hに属さないGの元aをとれば$aH\neq H$で，HとaHの2つが相異なる左剰余類の全体である．$a\notin H$からHaもHと異なり，$Ha\cap H=\phi$である（補題1.7）．$G=H\cup aH$からHaの元はすべてaHに属する．同じようなことを右剰余類で考えて$aH\subseteqq Ha$となり，$aH=Ha$が成り立つ．

Hに属する元aに対しては$aH=H=Ha$. したがって，Gのすべての元aに対して$aH=Ha$が成り立つ．

例1の(2)，例3の(a)は指数が2である．

例 6　Gを群とし,

$$S=\{aba^{-1}b^{-1} \mid a,b\in G\}$$

とおく. Sの元をGの**交換子**, Sから生成されたGの部分群(S)をGの**交換子群**とよぶ. このとき

交換子群を含むGの部分群は正規部分群である.

実際, (S)を含むGの部分群をH, Gの任意の元をaとすると, aHa^{-1}の任意の元aha^{-1}に対して$aha^{-1}h^{-1}\in S\subseteqq(S)\subseteqq H$であるから, $aha^{-1}\in Hh=H$となりHはGの正規部分群である.

補題 1.13　Gを群, HをGの正規部分群とする. a,bがGの元ならば, Hを法とする剰余類の(群の部分集合としての)積に関して

$$aH\cdot bH=abH$$

が成り立つ.

証明　群の部分集合の積に関して結合法則が成り立つから,

$$\begin{aligned}aH\cdot bH&=(aH\cdot b)H=(a\cdot Hb)H=(a\cdot bH)H=(ab\cdot H)H\\&=ab\cdot(HH)=abH\end{aligned}$$

である. ここで最後の等号は, 部分群Hに対して$HH=H$である(この証明は演習問題とする)ことによる.

群Gの正規部分群Hを法とする剰余類の全体をG/Hとかく. このG/Hが群をつくることを示す. 演算φを

$$\varphi\colon G/H\times G/H\to G/H,\quad (aH,bH)\to aH\cdot bH$$

ときめる. ここで$aH\cdot bH$は群Gの部分集合の積をあらわす. 補題1.13からabHとしてもよい.

まず, φが一意写像であることを確かめる. それには$aH=a'H$, $bH=b'H$ならば$abH=a'b'H$を示せばよい. 仮定から$a^{-1}a'\in H$, $b^{-1}b'\in H$で

$$(ab)^{-1}\cdot a'b'=b^{-1}\cdot a^{-1}a'\cdot b'\in b^{-1}Hb'=b^{-1}(b'H)=(b^{-1}b')H=H$$

が成り立つ. これは$abH=a'b'H$を意味する.

次に, G/Hの元aH,bH,cHに対して

$$(aH\cdot bH)\cdot cH=abH\cdot cH=(ab)cH,$$
$$aH\cdot(bH\cdot cH)=aH\cdot bcH=a(bc)H$$

であるから, G/Hは上のφに関して結合法則をみたす. G/Hの単位元は$eH=H$, G/Hの元aHの逆元は$a^{-1}H$である. したがって, G/Hは上のφに関し

て群をつくる.

定理 1.14 Gを群, HをGの正規部分群とする. Hを法とする剰余類の全体G/Hは2元aH, bHの積を$aH\cdot bH=abH$ときめて群をつくる.

この群をGのHによる**剰余群**とよぶ. $|G/H|$ は指数 $(G:H)$ に等しい.

例 7 加法群$\boldsymbol{Z}$はアーベル群で, その部分群 (m) (mは自然数) は正規部分群である. $\boldsymbol{Z}$の (m) による剰余群$\boldsymbol{Z}/(m)$はm個の剰余類

$$0+(m), 1+(m), 2+(m), \cdots, m-1+(m)$$

からなる群で, このm個の剰余類を$i+(m)=\bar{i}$とおいて, 簡単に

$$\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{m-1}$$

とかく.

$\boldsymbol{Z}/(m)$ の2元$\bar{i}, \bar{j}$ $(0\leqq i, j\leqq m-1)$ の和は

$$\bar{i}+\bar{j}=\overline{i+j}$$

である. しかし, $i+j\geqq m$となる場合もあり, そのとき$\overline{i+j}$は (形の上では) $\boldsymbol{Z}/(m)$ に属さない. そこで, $i+j$をmで割って

$$i+j=mq+r \qquad (0\leqq r<m)$$

とかけば, $m\,|\,(i+j)-r$であるから

$$\overline{i+j}=\bar{r}$$

となり, $0\leqq r<m$であるから$\overline{i+j}=\bar{r}$は$\boldsymbol{Z}/(m)$ に属する.

例えば, $m=6$のとき

$$\boldsymbol{Z}/(6)=\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$$

において$\bar{5}+\bar{4}=\overline{5+4}=\bar{9}$となる. 9を6で割って$9=6\times1+3$とかけば,

$$\bar{5}+\bar{4}=\bar{9}=\bar{3}$$

となる. $\boldsymbol{Z}/(6)$ の乗積表は表1.4のようになる. 右下の三角形の部分が$\bar{r}$を用いてあらわしたものである.

表 1.4

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

例 8　群Gの自明な部分群Gと$\{e\}$は正規部分群であった．1.3節でのべたように，Gを法とする剰余類はGだけで，したがって，剰余群G/Gは単位群である．

Gの元aの$\{e\}$を法とする剰余類は$\{a\}$で，剰余群$G/\{e\}$は

$$G/\{e\}=\{\{a\}\mid a\in G\}$$

で与えられる．このときaと$\{a\}$とを同一視して，Gと$G/\{e\}$とを同じものとみる（次節参照）．

例 9　Gを群，HをGの正規部分群，(S)をGの交換子群とする．このとき

$$\begin{aligned} G/H\text{がアーベル群} &\Leftrightarrow G\text{の任意の元}\ a,b\ \text{に対して}\ Hab=Hba \\ &\Leftrightarrow G\text{の任意の元}\ a,b\ \text{に対して}\ ab\cdot(ba)^{-1}\in H \\ &\Leftrightarrow S\subseteqq H \\ &\Leftrightarrow (S)\subseteqq H. \end{aligned}$$

すなわち，(S)は剰余群がアーベル群となる最小の正規部分群である．

1.4　群の準同型

群Gから群G'への一意写像$f: G\to G'$が，Gの任意の2元a,bに対して

$$f(a\cdot b)=f(a)\cdot f(b)$$

をみたすとき，fをGからG'への**準同型写像**または単に**準同型**とよぶ．ここで左辺の・はGにおける演算をあらわし，右辺の・は同じ・であるがG'における演算をあらわす．

準同型fが単射ならば，fを**単射準同型**，全射ならば**全射準同型**とよぶ．特に，全単射準同型fを**同型写像**または単に**同型**とよぶ．GからG'への同型fが存在するとき，GとG'は同型であるといい，$G\cong^f G'$または単に$G\cong G'$とあらわす．

補題 1.15　G, G'が群，$f: G\to G'$が準同型ならば，

(1)　Gの単位元eに対して，$f(e)$はG'の単位元e'に等しい．

(2)　Gの任意の元aに対して$f(a^{-1})=f(a)^{-1}$が成り立つ．

証明　(1)　Gの任意の元aに対して

$$f(a)\cdot f(e)=f(ae)=f(a)=f(a)\cdot e'$$

であるから，G'における左簡約律を用いて$f(e)=e'$となる．

(2)　Gの任意の元aに対して

$$f(a)\cdot f(a^{-1})=f(a\cdot a^{-1})=f(e)=e'=f(a)\cdot f(a)^{-1}$$

であるから，G' における左簡約律により $f(a^{-1})=f(a)^{-1}$ をうる．

補題 1.16　G, G', G'' を群とする．

(1)　$f: G\to G'$, $g: G'\to G''$ が共に準同型ならば，f と g を合成した写像 $gf: G\to G''$ も準同型である．

(2)　$f: G\to G'$ が同型ならば，逆写像 $f^{-1}: G'\to G$ も同型である．

証明　(1) は G の 2 元 a, b に対して

$$gf(ab)=g(f(ab))=g(f(a)\cdot f(b))=g(f(a))\cdot g(f(b))=gf(a)\cdot gf(b)$$

であることから明らか．

(2)　f が全射であるから，G' の任意の 2 元を $f(a), f(b)$ $(a, b\in G)$ とかく．このとき

$$f^{-1}(f(a)\cdot f(b))=f^{-1}(f(ab))=ab=f^{-1}(f(a))\cdot f^{-1}(f(b))$$

であるから，f^{-1} も準同型で，したがって，同型である．

例 1　正の実数の全体 $\boldsymbol{R}^{+}$ は乗法群 $\boldsymbol{R}^{*}$ の部分群である．乗法群 $\boldsymbol{C}^{*}$ からこの乗法群 $\boldsymbol{R}^{+}$ への写像 f を

$$f: \boldsymbol{C}^{*}\to\boldsymbol{R}^{+},\quad z\to|z|$$

ときめる．f は一意写像である．ここで $|z|$ は複素数 z の絶対値をあらわす．$\boldsymbol{C}^{*}$ の元 z, z' に対して $|zz'|=|z|\cdot|z'|$ であるから，f は準同型である．$\boldsymbol{R}^{+}$ の元 a に対して $|a|=a$ であるから，f は全射である．しかし，$\boldsymbol{C}^{*}$ の元 z に対して $|z|=|-z|$ であることは，f が単射ではないことを示している．

次の例は加法群から乗法群への準同型の例である．G が加法群，G' が乗法群であるとき，写像 $f: G\to G'$ が準同型であるとは，G の任意の 2 元 a, b に対して

$$f(a+b)=f(a)\cdot f(b)$$

が成り立つことを意味する．

例 2　G を群，a を G の元とする．加法群 $\boldsymbol{Z}$ から G への写像 f を

$$f: \boldsymbol{Z}\to G,\quad n\to a^{n}$$

ときめる．f は一意写像であり，$m, n\in\boldsymbol{Z}$ に対して定理 1.4 から $a^{m+n}=a^{m}\cdot a^{n}$ である．このことは $f(m+n)=f(m)\cdot f(n)$ を示し，f は $\boldsymbol{Z}$ から G への準同型であり，$\boldsymbol{Z}$ から (a) への準同型とみれば全射準同型である．ここで (a) は a から生成された G の巡回部分群をあらわす (1.2 節例 7)．

例 3　$a\ (\geqq 1)$ を実数として写像 f を

$$f: \boldsymbol{R}\to\boldsymbol{R}^{+},\quad x\to a^{x}$$

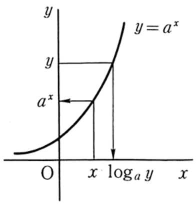


図 1.2

ときめる．f は一意写像である．$\boldsymbol{R}$ の元 x, y に対して $a^{x+y}=a^x\cdot a^y$ であるから，$f(x+y)=f(x)\cdot f(y)$ で f は加法群 $\boldsymbol{R}$ から乗法群 $\boldsymbol{R}^+$ への準同型である．

$a=1$ のときは，f は $\boldsymbol{R}$ のすべての元を実数 1 にうつす準同型である．$a>1$ ならば，図 1.2 の指数関数のグラフからも分かるように f は全単射である．実際，写像 g を

$$g:\boldsymbol{R}^+\to\boldsymbol{R},\quad y\to\log_a y$$

ときめれば，g は一意写像で

$$g(f(x))=\log_a a^x=x,\quad f(g(y))=a^{\log_a y}=y$$

であるから，g が f の逆写像であることが分かる．

例 4　G を群，H を G の正規部分群とし，G から剰余群 G/H への写像 π を

$$\pi: G\to G/H,\quad a\to aH$$

ときめる．π は一意写像である．G の 2 元 a, b に対して

$$aH\cdot bH=abH$$

であることは $\pi(ab)=\pi(a)\cdot\pi(b)$ を意味し，π は準同型である．π はまた全射でもある．この π を G から G/H への**標準的準同型**または**自然な準同型**とよぶ．

例 5　G を群とし，G の元 a を 1 個固定して写像 f_a を

$$f_a: G\to G,\quad x\to axa^{-1}$$

ときめる．f_a は一意写像である．G の元 x, y に対して $axya^{-1}=axa^{-1}\cdot aya^{-1}$ であることは $f_a(xy)=f_a(x)\cdot f_a(y)$ を意味し，f_a は準同型である．

$axa^{-1}=aya^{-1}$ であるとき，左から a^{-1}，右から a をかけて $x=y$ をうるが，これは f_a が単射であることを示す．一方，G の任意の元 y は $y=a(a^{-1}ya)a^{-1}$ とあらわされるから f_a は全射である．したがって，f_a は G から G への同型であり，G の置換である．この f_a の形の同型を特に G の**内部自己同型**とよぶ．

定理 1.17　G, G' を群，H, H' をそれぞれ G, G' の部分群とする．このとき

準同型$f: G \to G'$に対して

(1) fによるHの像$f(H)$はG'の部分群である．

(2) fによるH'の原像$f^{-1}(H')$はGの部分群である．

(3) $H' \lhd G' \Rightarrow f^{-1}(H') \lhd G$.

(4) fが全射で，$H \lhd G \Rightarrow f(H) \lhd G'$.

証明 ここでは(2)と(3)のみ証明する．残りは演習問題とする．

(2) $a, b \in f^{-1}(H')$ならば$f(a), f(b) \in H'$で

$$f(ab^{-1}) = f(a) \cdot f(b^{-1}) = f(a) \cdot f(b)^{-1} \in H'.$$

したがって，$ab^{-1} \in f^{-1}(H')$．Gの単位元eに対して$f(e)$はG'の単位元でH'に属するから，$e \in f^{-1}(H')$．定理1.5から$f^{-1}(H')$はGの部分群である．

(3) $a \in G, b \in f^{-1}(H')$ならば

$$f(aba^{-1}) = f(a)f(b)f(a)^{-1} \in f(a)H'f(a)^{-1} \subseteqq H'.$$

したがって，$aba^{-1} \in f^{-1}(H')$，$af^{-1}(H')a^{-1} \subseteqq f^{-1}(H')$である．定理1.12から$f^{-1}(H') \lhd G$である．

G, G'を群，$f: G \to G'$を準同型とする．fによるGの像$f(G)$を簡単にfの**像**とよぶ．これを$\mathrm{Im}\, f$ともかく．fが全射とは$f(G) = G'$を意味した．

G'の単位元e'に対して$H' = \{e'\}$はG'の正規部分群であり，$f^{-1}(H')$はGの正規部分群である．この$f^{-1}(H')$をfの**核**とよび，$\mathrm{Ker}\, f$であらわす．

$$\mathrm{Ker}\, f = \{a \in G \mid f(a) = e'\}.$$

Gの元a, bに対して

$$f(a) = f(b) \Leftrightarrow f(a)^{-1} \cdot f(b) = e' \Leftrightarrow a^{-1}b \in \mathrm{Ker}\, f$$

であるから

$$f\text{が単射} \Leftrightarrow \mathrm{Ker}\, f = \{e\}$$

である．また，$a^{-1}b \in \mathrm{Ker}\, f$は$\mathrm{Ker}\, f$を法とする$a$の剰余類$a \cdot \mathrm{Ker}\, f$と$b$の剰余類$b \cdot \mathrm{Ker}\, f$とが一致することを意味するから，$f$から誘導された準同型

$$\bar{f}: G/\mathrm{Ker}\, f \to G', \quad a \cdot \mathrm{Ker}\, f \to f(a)$$

は単射準同型である．$\bar{f}$の像は$f(G)$に等しいから次の定理が成り立つ．

定理 1.18（群の準同型定理） G, G'が群，$f: G \to G'$が準同型ならば，

$$G/\mathrm{Ker}\, f \overset{\bar{f}}{\cong} f(G).$$

例 6 例1の全射準同型$f: \boldsymbol{C}^* \to \boldsymbol{R}^+$の核は絶対値1の複素数の全体で，これを1.2節例3でTとかき，1次元のトーラス群とよんだ．Tはfの核であるから$\boldsymbol{C}^*/T \cong \boldsymbol{R}^+$が成り立つ．

実数の加法群 $\boldsymbol{R}$ から乗法群 T への写像 g を

$$g\colon \boldsymbol{R} \to T, \quad \alpha \to \cos 2\pi\alpha + i \sin 2\pi\alpha$$

ときめると，g は一意写像であり全射準同型であって，その核は $\boldsymbol{Z}$ に等しいから $\boldsymbol{R}/\boldsymbol{Z} \cong T$ でもある．

例 7　Gを群，aをGの元とする．例 2 の全射準同型

$$f\colon \boldsymbol{Z} \to (a), \quad n \to a^n$$

の核は $\mathrm{Ker}\, f = \{n \in \boldsymbol{Z} \mid a^n = e\}$ である．

$\mathrm{Ker}\, f = \{0\}$ ならば，f は単射で

$$\boldsymbol{Z} \cong^f (a)$$

である．このとき a の**位数**は無限であるという．

$\mathrm{Ker}\, f \neq \{0\}$ ならば，$\mathrm{Ker}\, f$ に属する最小の自然数 m があって $\mathrm{Ker}\, f = (m)$ が成り立つ (1.2 節例 10)．したがって，

$$\boldsymbol{Z}/(m) \cong^{\bar{f}} (a).$$

このとき m を a の**位数**とよぶ．

この定義から a の位数が無限のときは

$$a^n = e \Leftrightarrow n \in \mathrm{Ker}\, f = \{0\} \Leftrightarrow n = 0$$

であり，a の位数が m のときは

$$a^n = e \Leftrightarrow n \in \mathrm{Ker}\, f = (m) \Leftrightarrow m \mid n$$

が成り立つ．

上の同型対応から，a の位数が無限のとき

$$(a) = \{\cdots, a^{-2}, a^{-1}, a^0 = e, a, a^2, \cdots\}$$

で (a) の位数も無限であり，a の位数が m であるときは

$$(a) = \{a^0 = e, a, a^2, \cdots, a^{m-1}\}$$

で (a) の位数も m である．したがって，a の位数の有限，無限をとわず

$$a \text{ の位数} = (a) \text{ の位数}$$

である．

Gが有限群ならば，Gのどの元の位数も無限ではありえない．Gの元 a の位数を m とおけば，系 1.11 から (a) の位数 m は G の位数の約数であるから，$m \mid |G|$．したがって，

定理 1.19　有限群 G の任意の元 a に対して $a^{|G|} = e$.

例 8　Gを群，HをGの正規部分群とする．剰余群 G/H の単位元は $eH = H$ であるから，標準的準同型 $\pi\colon G \to G/H$ に対して

$$a \in \mathrm{Ker}\, \pi \Leftrightarrow aH = H \Leftrightarrow a \in H$$

(1.3 節参照). したがって,

$$\mathrm{Ker}\,\pi = H.$$

準同型 $f: G \to G'$ の核 $\mathrm{Ker}\,f$ は G の正規部分群であったが, 上の $\mathrm{Ker}\,\pi = H$ は, G の正規部分群はある準同型の核にほかならないことを示している.

G を群, H を G の正規部分群, K を H を含む G の部分群とする. このとき, H は群 K の正規部分群であるから, 剰余群 K/H がつくれる. この K/H から任意の元 bH をとる. b は K の元で bH は

$$bH = \{bx \in K \mid x \in H\} \qquad \cdots\cdots①$$

の形の K の部分集合である. ここで積 bx は K での積をあらわす.

K の元 b は G の元であるから, H を法とする G の元 b の剰余類

$$\{bx \in G \mid x \in H\} \qquad \cdots\cdots②$$

が考えられる. ここで積 bx は G における積をあらわす. しかし, K での積は G における積にほかならないから, この ①, ② の 2 つの集合は全く同じものである.

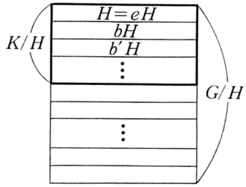


図 1.3

このことは, K を群, H を K の正規部分群とみて剰余群 K/H をつくれば, K/H は G/H の部分集合で, 集合として

$$K/H = \{bH \in G/H \mid b \in K\}$$

であることを意味している.

次の定理は, この記号を用いて, 剰余群 G/H の部分群を特徴づけている.

定理 1.20 G を群, H を G の正規部分群, $\pi: G \to G/H$ を標準的準同型とする. このとき

(1) G/H の任意の部分群 H' に対して, π による H' の原像 $\pi^{-1}(H')$ は H を含む G の部分群で,

$$H' = \pi^{-1}(H')/H.$$

(2)　Hを含むGの任意の部分群Kに対して

$$K/H=\{bH\in G/H \mid b\in K\}$$

はG/Hの部分群である．

(3)　G/Hの部分群H'とHを含むGの部分群Kとに対して

$$H' \to \pi^{-1}(H')$$
$$K/H \leftarrow K$$

はG/Hの部分群の全体とHを含むGの部分群の全体との間の全単射を与える．

(4)　(3)の対応で

$$K\lhd G \Leftrightarrow K/H\lhd G/H$$

であり，このとき

$$(G/H)/(K/H)\cong G/K$$

が成り立つ．

証明　(1),(2)は定理1.17から明らか．

(3)　$\pi^{-1}(H')/H=H'$と$\pi^{-1}(K/H)=K$を示せばよいが，第1式は(1)から，第2式は

$$aH\in K/H \Leftrightarrow \text{ある } k\in K \text{ があって } aH=kH \Leftrightarrow a\in K$$

からえられる．

(4)の前半は定理1.17から明らか．後半を示すには，写像fを

$$f: G/H\to G/K,\quad aH\to aK$$

ときめる．$H\subseteqq K$からfは一意写像で全射準同型にもなっている．

$$\mathrm{Ker}\, f=\{aH\in G/H \mid aK=K\}=\{aH\in G/H \mid a\in K\}=K/H$$

で，したがって，定理1.18から$(G/H)/(K/H)\cong G/K$をうる．

例 9　剰余群$\boldsymbol{Z}/(6)$の部分群をすべて求めてみよう．

まず，(6)を含む$\boldsymbol{Z}$の部分群(m)を求める．定理1.20から$\boldsymbol{Z}/(6)$の部分群はすべて$(m)/(6)$の形であらわされる．$(6)\subseteqq(m)$は$m|6$を意味し，mは自然数であるから，$m=1,2,3$または6である．$m=1,6$ならば，$(m)/(6)$はそれぞれ$\boldsymbol{Z}/(6)$, $(6)/(6)$で自明な部分群である．$\boldsymbol{Z}/(6)=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5}\}$であるから，自明でない部分群は

$$(2)/(6)=\{\bar{a}\in\boldsymbol{Z}/(6) \mid a\in(2)\}=\{\bar{0},\bar{2},\bar{4}\},$$
$$(3)/(6)=\{\bar{a}\in\boldsymbol{Z}/(6) \mid a\in(3)\}=\{\bar{0},\bar{3}\}$$

の2つである．

例 10　Gを群，a,bをGの元とする．Gのある内部自己同型によってaがbにうつされるとき，すなわち，$sas^{-1}=b$となるGの元sが存在するとき，a

は b に**共役**であるという．a が b に共役であるとき $a \sim b$ とかけば，$\sim$ は G の上の同値関係を与える．すなわち，G の元 a, b, c に対して

(1) $a \sim a$,

(2) $a \sim b \Rightarrow b \sim a$,

(3) $a \sim b, b \sim c \Rightarrow a \sim c$

が成り立つ．

(1) は $eae^{-1}=a$ であるから，(2) は $sas^{-1}=b$ ならば $s^{-1}b(s^{-1})^{-1}=a$ であるから，(3) は $sas^{-1}=b$, $tbt^{-1}=c$ ならば $(ts)a(ts)^{-1}=c$ であることから，分かる．

a と共役な G の元の全体を $K(a)$ とかく．

$$K(a)=\{xax^{-1} \mid x \in G\}.$$

$K(a)$ を a の**共役類**とよぶ．a の共役類が a のみよりなる G の元 a は

G の任意の元 x に対して $xax^{-1}=a$

をみたす．このような元 a の全体は G の部分群をつくる．これを G の**中心**とよび，$Z(G)$ であらわす．

$$Z(G)=\{a \in G \mid G \text{ の任意の元 } x \text{ に対して } ax=xa\}.$$

G が有限群ならば，a の共役類に含まれる相異なる元の個数は $(G:N(a))$ である（演習問題 31）ことに注意すれば，

$$|G|=|Z(G)|+\sum\nolimits_a (G:N(a))$$

が成り立つ．ここで $\sum_a$ は中心に属さない元 a の共役類のうち相異なるものすべてにわたっての和をあらわす．この等式を**類等式**とよんでいる．

例 11 位数が素数 p のべきである有限群を **p 群**とよぶ．類等式を用いて

位数が p^2 の p 群 G はアーベル群である

ことを確かめてみる．

まず類等式の $(G:N(a))$ は p^2 の約数である（定理 1.10）から p で割り切れる．したがって，類等式から $|Z(G)|$ が p で割り切れる．$|Z(G)|=p$ ならば，$Z(G)$ に属さない G の元 a があり，$N(a)$ は a と共に $Z(G)$ の元のすべてを含むから $|N(a)|=p^2$ で，したがって，$G=N(a)$ となる．これは $a \in Z(G)$ を意味して矛盾である．$|Z(G)|$ は p^2 であり，$Z(G)=G$ となる．G はアーベル群である．

1.5 巡 回 群

群 G が，ある G の元 a から生成された G の巡回部分群 (a) に一致するとき，G を**巡回群**，a を G の**生成元**とよぶ．$a^m a^n = a^{m+n} = a^n a^m$ であるから，巡回群

はアーベル群である．1.4 節例 7 から

定理 1.21　$G=(a)$ を巡回群とすると

(1)　G が無限群 $\Leftrightarrow$ a の位数は無限．

このとき，$G=\{\cdots, a^{-2}, a^{-1}, a^0=e, a, a^2, \cdots\}$．

(2)　G が位数 m の有限群 $\Leftrightarrow$ a の位数は m．

このとき，$G=\{a^0=e, a, a^2, \cdots, a^{m-1}\}$．

例 1　加法群 $\boldsymbol{Z}$ は 1 を生成元とする無限巡回群である．$\boldsymbol{Z}$ は -1 を生成元とする巡回群でもあり（1.2 節例 9），このことは巡回群の生成元が 1 個とはかぎらないことを示している．

例 2　自然数 m に対して，複素数 α を

$$\alpha=\cos\frac{2\pi}{m}+i\sin\frac{2\pi}{m}$$

ときめれば，$\alpha^m=1$ で

$$G=(\alpha)=\{1, \alpha, \alpha^2, \cdots, \alpha^{m-1}\}$$

は位数 m の巡回群をつくる．G は 1 の m 乗根の全体である．

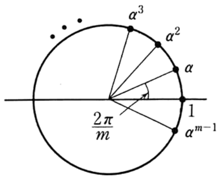


図 1.4

例 3　位数 4 の群 G は巡回群か，2 元から生成されたアーベル群である．

$G=\{e, a, b, c\}$（e は G の単位元）とする．a, b, c の中に位数 4 の元があれば，その元から生成された G の巡回部分群は G と一致し，G は巡回群である．a, b, c の中に位数 4 の元がないときは a, b, c の位数はすべて 2 である．したがって，

$$a^2=e,\quad a=a^{-1},\quad b^2=e,\quad b=b^{-1},\quad c^2=c,\quad c=c^{-1}$$

で，このとき積 ab は a, b とも e とも異なり，$ab=c$ でなければならない．

$$G=\{e, a, b, ab\}$$

で，G は 2 元 a, b から生成される．G がアーベル群であることは演習問題 3 からも分かる．この群 G を**クラインの 4 元群**とよんでいる．

巡回群 $G=(a)$ のすべての部分群を求めてみよう．$G\neq\{e\}$ とし 1.4 節例 2

の全射準同型 $f\colon \boldsymbol{Z}\to G$, $n\to a^n$ を考える．

$H\neq\{e\}$ を G の部分群とする．$e\neq a^m\in H$ がある．$m\neq 0$ から $f^{-1}(H)$ は $\{0\}$ と異なる $\boldsymbol{Z}$ の部分群である．$f^{-1}(H)=(s)$ をみたす自然数 s がきまる．

$$H=f(f^{-1}(H))=f((s))=(a^s)$$

で H は巡回群である．このとき，整数 n に対して

$$a^n\in H \Leftrightarrow n\in f^{-1}(H) \Leftrightarrow s|n$$

が成り立つ．

$H=\{e\}$ のときは $H=(e)$ でまた巡回群である．

したがって，巡回群の部分群はすべて巡回群である．

G が無限群のときは，無限個の部分群

$$(e), (a), (a^2), (a^3), \cdots$$

が存在する．もしある $i>0$ があって $(e)=(a^i)$ ならば，

$$a^i\in(e),\quad a^i=e$$

となり，a の位数が無限であることに反する．また，もし $(a^i)=(a^j)$ $(0<i<j)$ をみたす i,j があれば，$a^i\in(a^j)$．ある整数 k に対して

$$a^i=a^{kj},\quad a^{i-kj}=e.$$

1.4 節例 7 から $i-kj=0$．このとき $k>0$ から $j>i=kj\geqq j$ となって矛盾を生ずる．したがって，上の無限個の部分群はすべて相異なり，またこの無限個の部分群が G の部分群のすべてをつくしている．

G が位数 m の有限群とする．部分群 $H\neq\{e\}$ に対して，$H=(a^s)$ をみたす自然数 s が存在する．定理 1.19 から $a^m=e\in H$ であり，上に注意したように $s|m$ で s は m の正の約数であり，m とは異なる．このとき $m=st$ とかけば，

$$(a^s)^t=a^{st}=a^m=e$$

から a^s の位数も有限で，a^s の位数を k とすると $k|t$ である．一方，$a^{sk}=e$ で，a の位数が m であるから

$$m|sk,\quad t|k$$

となって $t=k$ をうる．すなわち，H は位数 t の部分群で

$$H=\{a^0=e, a^s, a^{2s}, \cdots, a^{(t-1)s}\}$$

が成り立つ．このとき

$$H=\{x\in G|\ x^t=e\}$$

でもある．この証明は演習問題とする．

m の正の約数で相異なるもののすべてを $1, s_1, s_2, \cdots, s_h, m$ とかけば，

$$(e), (a^{s_h}), \cdots, (a^{s_2}), (a^{s_1}), (a)$$

がGの相異なる部分群のすべてをつくすことが分かる．

以上をまとめて

定理 1.22　巡回群の部分群はまた巡回群である．

$G=(a)$ が巡回群で無限群のときは

$$(e), (a), (a^2), \cdots$$

がGの相異なる部分群のすべてをつくす．

$G=(a)$ が巡回群で位数 m の有限群のときは，m の正の約数で相異なるもののすべてを $1, s_1, s_2, \cdots, s_h, m$ とかけば，

$$(e), (a^{s_h}), \cdots, (a^{s_2}), (a^{s_1}), (a)$$

が相異なるGの部分群のすべてをつくす．

例 4　群Gが単位群でないならば，

$$G\text{の位数は素数} \Leftrightarrow G\text{は自明な部分群しかもたない．}$$

このとき，Gは巡回群である．

実際，Gの位数が素数 p ならば，部分群の位数は1か p で（系1.11），Gは自明な部分群しかもたない．逆に，Gが自明な部分群しかもたないならば，$G\ni a\neq e$ に対して $G=(a)$ である．Gは有限群で，その位数は正の約数を2つしかもたないから素数である．

例 5　$G=(a)$ が有限巡回群，H, K がGの部分群ならば，

$$H\subseteqq K \Leftrightarrow |H|\,|\,|K|.$$

実際，HがKの部分群ならば，$|H|\,|\,|K|$ は系1.11から明らか．

逆に，Gの位数を m とし，$|H|\,|\,|K|$ とする．$K=(a^s), H=(a^{s'})$ とおく．s, s' は m の正の約数で $m=st, m=s't'$ とかく．このとき，$|K|=t, |H|=t'$ であったから，$t=t'k$ をみたす自然数 k があり，したがって，$s't'=st=st'k$ から $s'=sk$，$a^{s'}=(a^s)^k\in K$ となり，$H\subseteqq K$ をうる．

再び整数に関するいくつかの注意をのべる．

a, b が整数で，a が b を割り切るとき $a|b$ とかいた．そうでないときは $a\nmid b$ とかくことにする．

整数 $a_1, a_2, \cdots, a_n$ に対して

$$d|a_1, d|a_2, \cdots, d|a_n$$

をみたす整数 d $(\neq 0)$ を $a_1, a_2, \cdots, a_n$ の**公約数**とよぶ．例えば，1とか -1 はいつも公約数である．

$a_1, a_2, \cdots, a_n$ の公約数の中に最大なものがあれば，それを $a_1, a_2, \cdots, a_n$ の**最**

大公約数とよぶ．最大公約数は，もしあれば，1より小さくないから自然数であり，最大という意味で一意的にきまる．

$a_1, a_2, \cdots, a_n$ の中に0でないものがあるとする．$S=\{a_1, a_2, \cdots, a_n\}$ から生成された加法群 $\boldsymbol{Z}$ の部分群 (S) は

$$(S)=\{m_1a_1+m_2a_2+\cdots+m_na_n \mid m_1, m_2, \cdots, m_n \in \boldsymbol{Z}\}$$

で与えられる（1.2 節例 9）．$(S) \neq \{0\}$ から $(S)=(d)$ をみたす自然数 d が存在する．

(d) が $a_1, a_2, \cdots a_n$ のすべてを含むから，d は $a_1, a_2, \cdots, a_n$ の公約数である．$a_1, a_2, \cdots, a_n$ の任意の公約数 d' に対して，(d') は $a_1, a_2, \cdots, a_n$ のすべてを含む $\boldsymbol{Z}$ の部分群であるから，$(S) \subseteqq (d')$ が成り立つ．したがって，$(d) \subseteqq (d')$．ある整数 q があって $d=d'q$ とかける．$d'<0$ のときは $d'<d$ であり，$d'>0$ のときは $d=d'q \geqq d'$ である．したがって，d は $a_1, a_2, \cdots, a_n$ の最大公約数である．

(1) 整数 $a_1, a_2, \cdots, a_n$ の中に0でないものがあれば，$a_1, a_2, \cdots, a_n$ の最大公約数 d が存在して

$$d=m_1a_1+m_2a_2+\cdots+m_na_n \qquad (m_1, m_2, \cdots, m_n \in \boldsymbol{Z})$$

とあらわされる．

2つの整数 a, b の最大公約数が1のとき，a, b を**互いに素**という．このとき，(1) から $ma+nb=1$ をみたす整数 m, n がある．逆に，$ma+nb=1$ ならば，$S=\{a, b\}$ に対して $(S)=(1)$．a, b の中に0でないものがあるから a, b の最大公約数 d が存在して $(d)=(S)=(1)$．したがって，$d=1$．

(2) 整数 a, b が互いに素 $\Leftrightarrow$ ある整数 m, n があって $ma+nb=1$.

2つの整数 a, b の最大公約数を (a, b) とかく．a, b, p が整数で，$(a, p)=1$，$(b, p)=1$ とすると，

$$ma+np=1, \quad ub+vp=1$$

をみたす整数 m, n, u, v が存在する．このとき

$$1=(ma+np)(ub+vp)=(mu)ab+((mv)a+(nu)b+(nv)p)p$$

であるから，$(ab, p)=1$ となる．

特に，p が素数ならば

$$(a, p)=1 \Leftrightarrow p \nmid a$$

であるから，上のことは

$$p \nmid a \text{ かつ } p \nmid b \Rightarrow p \nmid ab,$$

または，対偶をとって

$$p|ab \Rightarrow p|a \text{ または } p|b$$

を意味する．

整数 $a_1, a_2, \cdots, a_n$ に対して

$$a_1|l, a_2|l, \cdots, a_n|l$$

をみたす整数 l を $a_1, a_2, \cdots, a_n$ の**公倍数**とよぶ．したがって，$a_1, a_2, \cdots, a_n$ の公倍数が存在するためには，$a_1, a_2, \cdots, a_n$ の中に 0 となるものがあってはならない．l が $a_1, a_2, \cdots, a_n$ の公倍数ならば，$-l$ も公倍数であるから，$a_1, a_2, \cdots, a_n$ の公倍数が存在すれば正の公倍数があり，これら正の公倍数全体の集合の中には最小数が存在する(1.2 節参照)．この最小数を $a_1, a_2, \cdots, a_n$ の**最小公倍数**とよぶ．$a_1, a_2, \cdots, a_n$ のすべてが 0 でなければ，積 $a_1a_2\cdots a_n$ は $a_1, a_2, \cdots, a_n$ の公倍数であり，したがって，$a_1, a_2, \cdots, a_n$ の最小公倍数が存在する．

このとき，a_1 から生成された加法群 $\boldsymbol{Z}$ の巡回部分群 (a_1), a_2 から生成された加法群 $\boldsymbol{Z}$ の巡回部分群 $(a_2), \cdots$ に対して，共通部分 $(a_1)\cap(a_2)\cap\cdots\cap(a_n)$ は積 $a_1a_2\cdots a_n\neq 0$ を含んで $\{0\}$ ではない $\boldsymbol{Z}$ の部分群であるから，

$$(a_1)\cap(a_2)\cap\cdots\cap(a_n)=(l)$$

をみたす自然数 l がある．この l が $a_1, a_2, \cdots, a_n$ の最小公倍数であることは，最大公約数のときと同じように証明できる．

(3) 最小公倍数と最大公約数との間には

a, b が自然数，その最大公約数を d，最小公倍数を l とかけば，

$$ab=dl$$

の関係がある．

実際，$a=da', b=db'$ とかけば，a', b' は互いに素である．このとき $a'b=da'b'$ は a, b の正の公倍数である．

k を a, b の正の公倍数とし，$k=ax, k=by$ とかく．$da'x=k=db'y, a'x=b'y$ で $a'|b'y$．a', b' が互いに素であるから $a'|y$．したがって，$a'b|by, a'b|k$ となる．これから $k\geqq a'b$ をうるから $l=a'b$ で $ab=dl$ となる．

例 6　$G=(a)$ が有限巡回群，H, K が G の部分群であるならば，

$$|H\cap K|=|H|, |K| \text{ の最大公約数},$$
$$|HK|=|H|, |K| \text{ の最小公倍数}.$$

G の位数を m とおく．$|H\cap K|$ は例 5 から $|H|, |K|$ の公約数である．d を $|H|, |K|$ の任意の正の公約数とする．$d\,|\,|H|, |H|\,|\,m$ から $d|m$．$m=ds$ とかけば，(a^s) は位数 d の G の部分群で，例 5 から $(a^s)\subseteqq H$．同じようにして，$(a^s)\subseteqq K$ で $(a^s)\subseteqq H\cap K$．したがって，$d\,|\,|H\cap K|$ で $|H\cap K|\geqq d$ をうる．このこ

とは $|H\cap K|$ が $|H|, |K|$ の最大公約数であることを示している．

演習問題30によって $K/H\cap K\cong HK/H$ であるから，$(K:H\cap K)=(HK:H)$．定理1.10から $\dfrac{|K|}{|H\cap K|}=\dfrac{|HK|}{|H|}$．したがって，$|H|\cdot|K|=|H\cap K|\cdot|HK|$．この式と上の(3)から後半のことが分かる．

巡回群の生成元が一通りとはかぎらないことはすでに注意した．いかなる元が生成元となりうるかを調べてみる．

$G=(a)$ を巡回群とする．a^s が G の生成元ならば $a\in G=(a^s)$ から

$$a=a^{st},\quad a^{st-1}=e$$

をみたす整数 t が存在する．逆に，このような t があれば a^s は G の生成元である．

G が無限群のときは

$$st-1=0,\quad s=\pm 1.$$

このとき，G の生成元は a か a^{-1} である．

G が位数 $m\ (>1)$ の有限群のときは

$$m\,|\,(st-1),\quad st+mx=1$$

をみたす整数 x が存在して，s と m は互いに素である．この逆も成り立って，

定理 1.23 巡回群 $G=(a)$ が

(1) 無限群ならば，G の生成元は a か a^{-1} である．

(2) 位数 $m\ (>1)$ の有限群ならば，$1\leqq s\leqq m-1$ に対して

$$a^s \text{ が } G \text{ の生成元} \Leftrightarrow s \text{ と } m \text{ が互いに素}.$$

自然数 m に対して，$1, 2, \cdots, m$ のうち m と互いに素であるものの個数を $\varphi(m)$ とかき，自然数の上で定義されたこの関数を**オイラーの関数**とよぶ．

$$\varphi(1)=\varphi(2)=1,\quad \varphi(3)=\varphi(4)=2,$$

$$\varphi(5)=4,\quad \varphi(6)=2,\quad \varphi(7)=6, \cdots$$

等である．定理1.23は位数 $m\ (>1)$ の巡回群の生成元の個数が $\varphi(m)$ に等しいことをのべている．このことは $m=1$ のときも成り立つ．

例 7 1の4乗根は $1, -1, i, -i$ の4個あって巡回群 (i) をつくっている (1.2節例8)．この中で -1 は4乗しなくても，2乗してすでに1であるが，i と $-i$ とは4乗してはじめて1となる．

一般に，1の m 乗根のうち，m 乗してはじめて1となるもの，すなわち，位

数がmの1のm乗根を1の**原始 m 乗根**とよぶ.

1のm乗根の全体は，$\alpha=\cos\dfrac{2\pi}{m}+i\sin\dfrac{2\pi}{m}$ とおけば，巡回群(α)で与えられる(例2). 1の原始m乗根は(α)の生成元で$\varphi(m)$個存在する.

$m=3$のときは$\alpha=\cos\dfrac{2\pi}{3}+i\sin\dfrac{2\pi}{3}=-\dfrac{1}{2}+\dfrac{\sqrt{3}}{2}i$であり，これを$\omega$とかけば$\omega$は1の原始3乗根で

$$\omega\neq 1,\quad \omega^2=\frac{-1-\sqrt{3}i}{2}\neq 1,\quad \omega^3=1$$

と3乗してはじめて1となる. $\varphi(3)=2$でω,ω^2が1の原始3乗根をつくす.

$m=4$のときは$\alpha=\cos\dfrac{\pi}{2}+i\sin\dfrac{\pi}{2}=i$であり，1の原始4乗根は$\varphi(4)=2$個あって，$i,-i$が巡回群$(i)$の生成元をなす.

例 8　mを自然数とする. 加法群$\boldsymbol{Z}$の(m)による剰余群

$$\boldsymbol{Z}/(m)=\{\bar{0},\bar{1},\bar{2},\cdots,\overline{m-1}\}\qquad (\bar{i}=i+(m))$$

は$\bar{1}$を生成元とする巡回群である. この巡回群の生成元をmを法とする**既約剰余類**とよんでいる. 定理1.23からmを法とする既約剰余類は$\varphi(m)$個ある.

一般に，$\boldsymbol{Z}$の2元a,bに対して

$$a\equiv b \pmod m \Rightarrow (a,m)=(b,m)$$

である(この証明は演習問題とする)から，$\bar{s}$が既約剰余類ならばsだけにかぎらず$\bar{s}$に属するすべての整数がmと互いに素になっている. ここで(a,m), (b,m)は最大公約数をあらわす.

mを法とする既約剰余類の全体をGとかき，Gに演算をきめる.

まず，整数i,jに対して

$$(i,m)=1,\ (j,m)=1 \Rightarrow (ij,m)=1$$

であり，また整数i',j'に対して$i\equiv i' \pmod m$，$j\equiv j' \pmod m$ならば,

$$ij-i'j'=i(j-j')+(i-i')j'$$

で，$i-i',j-j'$共に(m)に属するから$ij-i'j'$も(m)に属する. したがって，写像

$$\psi: G\times G\to G,\quad (\bar{i},\bar{j})\to\overline{ij}$$

は一意写像である. このψで既約剰余類$\bar{i}$と$\bar{j}$の積を

$$\bar{i}\cdot\bar{j}=\overline{ij}$$

ときめる.

Gがψに関して結合法則をみたすことは明らかであるから，右簡約律をみたすことを確かめる. $\bar{i}\bar{k}=\bar{j}\bar{k}$を仮定する. $m|ik-jk=(i-j)k$で，kとmは互い

に素．したがって，$m|i-j$, $\bar{i}=\bar{j}$. 同じようにGは左簡約律をみたす．定理1.3によりGは群，明らかにアーベル群となる．

Gの単位元は$\bar{1}$で，Gの位数が$\varphi(m)$であるから，任意の既約剰余類$\bar{i}$に対して

$$\bar{i}^{\varphi(m)}=\bar{1}, \quad i^{\varphi(m)}\equiv 1 \pmod{m}.$$

aとmを互いに素な整数とし，aをmで割って$a=mq+r$ $(0\leqq r<m)$とかく．$r\neq 0$でありmと互いに素であるから，$\bar{r}$はmを法とする既約剰余類である．$\bar{a}=\bar{r}$であるから

$$a^{\varphi(m)}\equiv 1 \pmod{m}$$

が成り立つ．これを**オイラーの定理**とよんでいる．

特にmが素数pのとき，$1, 2, \cdots, p$の中でpと互いに素なものは$1, 2, \cdots, p-1$の$(p-1)$個あるから$\varphi(p)=p-1$. このことから次の**フェルマーの定理**をうる．

定理 1.24 pを素数，aをpと互いに素な整数とすると，

$$a^{p-1}\equiv 1 \pmod{p}.$$

定理の式の両辺にaをかけて，$a^p\equiv a \pmod{p}$をうる．aがpと互いに素でないときは，$p|a$で$a\equiv 0 \pmod{p}$, $a^p\equiv 0 \pmod{p}$であるから，このときも$a^p\equiv a \pmod{p}$が成り立つ．したがって，

$$\text{任意の整数}\ a\ \text{に対して}\ a^p\equiv a \pmod{p}$$

である．

1.6 置換群

n次の対称群S_n（1.1節例6）は，n個の元からなる集合Xの置換全体のつくる群である．簡単に$X=\{1, 2, \cdots, n\}$と考える．

S_nの元σはXからXへの全単射であり，Xの元iをXのある元$\sigma(i)$にうつす．iに対して$\sigma(i)$は一意的にきまる．σは単射であるから，異なったi, jに対して$\sigma(i)$と$\sigma(j)$とは異なる．したがって，$\sigma(1), \sigma(2), \cdots, \sigma(n)$は相異なる$n$個の$X$の元で，全体として$1, 2, \cdots, n$と一致する．$\sigma(1), \sigma(2), \cdots, \sigma(n)$は，$1, 2, \cdots, n$を並べかえた1つの順列をあらわす．

S_nの元σを，1.1節例6のように

$$\sigma=\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

であらわす．S_n の元 σ, τ が等しいとは，σ, τ が写像であるから

$$\sigma(i)=\tau(i) \qquad (1\leqq i\leqq n)$$

を意味する．したがって，例えば，$n=3$ のとき

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 3 & 2 & 1 \\ 2 & 1 & 3 \end{pmatrix}$$

の3つは，あらわし方はちがっていても同じ置換，1を3に，2を1に，3を2にうつす置換をあらわしている．

σ には順列 $\sigma(1), \sigma(2), \cdots, \sigma(n)$ を，$1, 2, \cdots, n$ の順列 $i_1, i_2, \cdots, i_n$ には $\sigma=\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$ を対応させて，S_n と $1, 2, \cdots, n$ の順列全体との間の全単射がえられる．$1, 2, \cdots, n$ の順列は全部で $n!$ 個あるから，S_n の位数も $n!$ である．

S_n の単位元 e は X の恒等写像

$$e=\begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

であり，S_n の元 σ に対して，$\sigma(i)$ を i にうつす置換が σ の逆元 σ^{-1} である．

$$\sigma^{-1}=\begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

例えば，$\sigma=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ ならば

$$\sigma^{-1}=\begin{pmatrix} 3 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix}=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

S_n の2元 σ, τ に対して，σ と τ の積 $\tau\sigma$ は σ と τ の合成写像である．

$$\tau\sigma=\begin{pmatrix} 1 & 2 & \cdots & n \\ \tau\sigma(1) & \tau\sigma(2) & \cdots & \tau\sigma(n) \end{pmatrix}.$$

例えば，$\sigma=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$，$\tau=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ ならば

$$\tau\sigma=\begin{pmatrix} 1 & 2 & 3 \\ \tau\sigma(1) & \tau\sigma(2) & \tau\sigma(3) \end{pmatrix}=\begin{pmatrix} 1 & 2 & 3 \\ \tau(3) & \tau(1) & \tau(2) \end{pmatrix}=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$\sigma\tau=\begin{pmatrix} 1 & 2 & 3 \\ \sigma\tau(1) & \sigma\tau(2) & \sigma\tau(3) \end{pmatrix}=\begin{pmatrix} 1 & 2 & 3 \\ \sigma(3) & \sigma(2) & \sigma(1) \end{pmatrix}=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

で，$\tau\sigma$ と $\sigma\tau$ とが一致しないから，S_n は一般にはアーベル群ではない．

S_nの元σが，Xの異なった元$i_1, i_2, \cdots, i_s$に対して

$$\sigma(i_1)=i_2, \quad \sigma(i_2)=i_3, \quad \cdots, \quad \sigma(i_{s-1})=i_s, \quad \sigma(i_s)=i_1$$

をみたし，$i_1, i_2, \cdots, i_s$とは異なったXの元iに対しては

$$\sigma(i)=i$$

をみたすとき，すなわち，

$$\sigma=\begin{pmatrix} i_1 & i_2 & \cdots & i_{s-1} & i_s & i & j & \cdots \\ i_2 & i_3 & \cdots & i_s & i_1 & i & j & \cdots \end{pmatrix}$$

のとき，σをs次の**巡回置換**とよび，

$$\sigma=(i_1\ i_2\ \cdots\ i_s)$$

とかく．例えば，$n=3$として

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}=(1\ 2), \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}=(1\ 3\ 2).$$

1次の巡回置換とは恒等写像であるときめる．また，2次の巡回置換を**互換**とよぶ．したがって，互換とは$1, 2, \cdots, n$のうち2個の元を交換し，他の元を動かさないようなXの置換である．

補題 1.25 S_nの元は共通なXの元をもたないいくつかの巡回置換の積に分解される．この分解は順序を除いて一意的である．

証明 S_nの元σによって動くXの元がないときは，σは恒等写像で1次の巡回置換である．σによって動くXの元があれば，その最小の元をi_1とし，$\sigma(i_1)=i_2$とかく．$i_1 \neq i_2$である．$\sigma(i_2)=i_3$とかく．i_3がi_1ともi_2とも異なるときは$\sigma(i_3)=i_4$とかく．i_4がi_1, i_2, i_3のいずれとも異なるときは$\sigma(i_4)=i_5$とかく．この手続きをくりかえすと$i_1, i_2, i_3, \cdots$と相異なるXの元の列ができる．Xの元はもともとn個しかないから，この列がいつまでも続くことはありえない．$i_1, i_2, \cdots, i_s$は相異なり，i_{s+1}が$i_1, i_2, \cdots, i_s$のいずれかと一致したとする．もし

$$i_{s+1}=i_m \qquad (2 \leqq m \leqq s)$$

ならば，$\sigma(i_s)=i_{s+1}=i_m=\sigma(i_{m-1})$で$\sigma$が単射であることから

$$i_s=i_{m-1} \qquad (1 \leqq m-1 \leqq s-1)$$

となって矛盾である．したがって，

$$i_{s+1}=i_1, \quad \sigma(i_s)=i_{s+1}=i_1$$

でなければならない．

$i_1, i_2, \cdots, i_s$以外にσによって動くXの元があれば，その最小のものをj_1として同じことをくりかえす．この手続きをσによって動くXの元がなくなるま

でおこなえば，σ は

$$\sigma=\cdots\cdot(j_1\,j_2\cdots j_t)(i_1\,i_2\cdots i_s)$$

のように分解される．

一意性を示すために，σ が共通な X の元をもたない巡回置換の積として

$$\sigma=\sigma_1\,\sigma_2\cdots\sigma_l=\tau_1\,\tau_2\cdots\tau_m \qquad (l\leqq m)$$

と二通りに分解されたとする．ここでいずれの σ_i, τ_j も恒等置換ではないものとする．

$$\sigma_1=(k_1\,k_2\cdots k_s)$$

とおき，簡単のため $k_1, k_2, \cdots, k_s$ を σ_1 に属する X の元とよぶ．これらの元に対しては $\sigma(k_i)=\sigma_1(k_i)$ が成り立つ．

k_1 は σ で動くから $\tau_1, \tau_2, \cdots, \tau_m$ のいずれか1つに属する．それを τ_1 とする．$\tau_1, \tau_2, \cdots, \tau_m$ は交換可能であるから，この仮定で一般性を失うことはない．このとき $\tau_1(k_1)=\sigma(k_1)=\sigma_1(k_1)=k_2$ が成り立つ．τ_1 は巡回置換であるから k_2 も τ_1 に属し，$\tau_1(k_2)=\sigma(k_2)=\sigma_1(k_2)=k_3$．したがって，$k_3$ も τ_1 に属する．こうして $k_1, k_2, \cdots, k_s$ のすべてが τ_1 に属する．その上，$\tau_1(k_s)=\sigma(k_s)=\sigma_1(k_s)=k_1$ が成り立つ．

このように $\sigma_1, \sigma_2, \cdots, \sigma_l$ のそれぞれに対して，同じ X の元が属する $\tau_1, \tau_2, \cdots, \tau_l$ がきまる．τ_1 が $k_1, k_2, \cdots, k_s$ と異なる X の元 k を動かすならば，k は σ で動くから $\sigma_2, \sigma_3, \cdots, \sigma_l$ のいずれか1つに属する．仮に k が σ_2 に属するならば，k は τ_2 にも属することになり，τ_1, τ_2 は共通な X の元をもって矛盾を生ずる．したがって，

$$\tau_1=(k_1\,k_2\cdots k_s)=\sigma_1.$$

$\tau_2, \tau_3, \cdots, \tau_l$ についても同様であり，また $l=m$ でもある．

例 1
$$\sigma=\begin{pmatrix}1&2&3&4&5\\3&5&1&2&4\end{pmatrix}$$

では σ によって動く X の元の中で最小のものは1で，1が3に，その3が1にうつる．このことを簡単に 1→3→1 とかこう．

1, 3 以外にも σ によって動く X の元があり，その中の最小のものは2で，2→5→4→2 とうつる．1, 3, 2, 5, 4 以外に動く X の元はないから

$$\sigma=(2\ \ 5\ \ 4)(1\ \ 3)$$

とかける．実際，右辺の積 (2　5　4)(1　3) を念のため確かめてみると，

1は (1　3) で3にうつり，3は (2　5　4) で動かないから 1→3,

2は (1　3) で動かないで，(2　5　4) で5にうつるから 2→5,

同じようにして，3→1, 4→2, 5→4 であって (2　5　4)(1　3) は σ に一致する.

一般に，巡回置換は

$$(i_1\, i_2 \cdots i_s) = (i_1\, i_s)(i_1\, i_{s-1}) \cdots (i_1\, i_3)(i_1\, i_2)$$

と互換の積に分解できる（証明は演習問題とする）から，次の定理が成り立つ.

定理 1.26　S_n の元はいくつかの互換の積としてあらわされる．また，(1　k) ($2 \leqq k \leqq n$) の形の互換の積としてもあらわされる.

証明　後半の証明は $a \neq 1, b \neq 1$ ならば

$$(a\ \ b) = (1\ \ a)(1\ \ b)(1\ \ a)$$

とかけることに注意したらよい.

例 2　1.1 節例 6 の S_3 の各元は

$$a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ \ 2\ \ 3) = (1\ \ 3)(1\ \ 2),$$

$$b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ \ 3\ \ 2) = (1\ \ 2)(1\ \ 3),$$

$$u = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\ \ 3), \qquad v = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ \ 3),$$

$$w = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ \ 2)$$

とあらわされる.

$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ は 1 次の巡回置換と約束したが，例えば，$e = (1\ \ 2)(1\ \ 2)$ ともかける.

1.1 節例 6 の乗積表から

$$b = a^2, \quad w = au, \quad v = bu = a^2u,$$

$$a^3 = e, \quad u^2 = e, \quad (au)^2 = e$$

で，S_3 は a, u の 2 元から生成されている.

$$S_3 = \{e, a, a^2, u, au, a^2u\}.$$

逆に，群 G が位数 3 の元 a と位数 2 の元 u を含み，au の位数が 2 であるならば，a, u から生成された G の部分群 H は S_3 と同型である.

実際，H は $\{e, a, a^2, u, au, a^2u\}$ で，6 個の元からなる G の部分群である．その乗積表（表 1.5）をつくると S_3 と同型なことが分かる．ここで $auau = e$ から a^2 を左に，u を右にかけて $ua = a^2u$ であることに注意.

表 1.5

	e	a	a^2	u	au	a^2u
e	e	a	a^2	u	au	a^2u
a	a	a^2	e	au	a^2u	u
a^2	a^2	e	a	a^2u	u	au
u	u	a^2u	au	e	a^2	a
au	au	u	a^2u	a	e	a^2
a^2u	a^2u	au	u	a^2	a	e

定理 1.26 から S_n の元はすべて互換の積としてあらわされるが，そのあらわし方は，例えば，

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 3 & 5 & 1 & 2 & 4\end{pmatrix}=(2\ \ 4)(2\ \ 5)(1\ \ 3)=(2\ \ 4)(1\ \ 2)(2\ \ 5)(5\ \ 3)(5\ \ 1)$$

のようにかならずしも一通りではない．しかし，このあらわし方では，いずれも互換の個数は奇数である．このように互換の個数が偶数であるか奇数であるかは，あらわし方に無関係であることを証明することができる．

定理 1.27　S_n の元 σ を互換の積としてあらわすとき，互換の個数が偶数であるか奇数であるかはあらわし方に無関係に σ によってきまる．

証明　n 個の文字 $x_1, x_2, \cdots, x_n$ の**差積** $F(x_1, x_2, \cdots, x_n)$ を積

$$\begin{aligned}(x_1-x_2)(x_1-x_3)\cdots(x_1-x_{n-1})&(x_1-x_n)\\ (x_2-x_3)\cdots(x_2-x_{n-1})&(x_2-x_n)\\ \cdots\ \cdots&\\ (x_{n-2}-x_{n-1})&(x_{n-2}-x_n)\\ &(x_{n-1}-x_n)\end{aligned}$$

ときめ，x_i の添え字 i に σ を施したものを

$$\sigma(F(x_1, x_2, \cdots, x_n))=F(x_{\sigma(1)}, x_{\sigma(2)}, \cdots, x_{\sigma(n)})$$

とかく．特に，σ が互換 $(i\ j)$ $(i<j)$ のとき $\sigma(F(x_1, x_2, \cdots, x_n))$ は $F(x_1, x_2, \cdots, x_n)$ で x_i と x_j とを交換したものである．この交換によって $F(x_1, x_2, \cdots, x_n)$ にどのような変化がおこるかをみるために，差積の中で必要なところをぬきだしてかいてみる(図 1.5)．

x_i と x_j を交換すると，図 1.5 の (1), (2) の部分，(3), (4) の部分，(5), (6) の部分がそれぞれ入れかわり，全体として

$$\sigma(F(x_1, x_2, \cdots, x_n))=-F(x_1, x_2, \cdots, x_n)$$

となる．したがって，σ が偶数個の互換の積であれば，そのあらわし方がどう

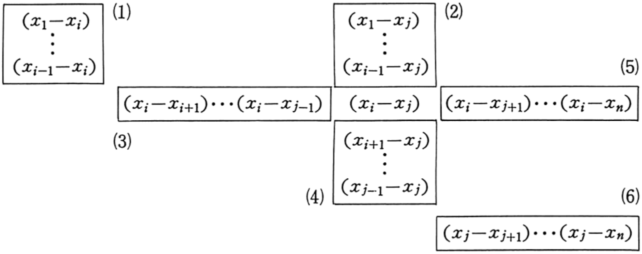


図 1.5

あっても $\sigma(F(x_1, x_2, \cdots, x_n)=F(x_1, x_2, \cdots, x_n)$ であり，奇数個の互換の積ならば $\sigma(F(x_1, x_2, \cdots, x_n))=-F(x_1, x_2, \cdots, x_n)$ である．このことから σ が，一方では偶数個の互換の積としてあらわされ，他方では奇数個の互換の積としてあらわされるということはおこりえない．

偶数個の互換の積としてあらわされる S_n の元を**偶置換**，奇数個の互換の積としてあらわされる S_n の元を**奇置換**とよぶ．

S_n の元 σ において

$$i<j \text{ で，かつ } \sigma(i)>\sigma(j)$$

である X の元の組 (i,j) があるとき，これを σ の**転位**とよぶ．このとき σ に互換 $(\sigma(i)\ \sigma(j))$ をかければ (i,j) の間の転位は消える．したがって，転位の数だけの互換を σ にかけて σ を恒等置換にすることができる．

例 3
$$\sigma=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$$

では $(1,2), (1,3)$ の間に 2 個の転位がある．まず，互換 $(\sigma(1)\ \sigma(2))$ を σ にかけて

$$\tau=(\sigma(1)\ \sigma(2))\cdot\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}=\begin{pmatrix}1 & 1 & 3\\ 1 & 3 & 2\end{pmatrix}$$

とする．σ の $(1,3)$ の間の転位は τ では $(2,3)$ の間の転位にかわる．

$$(\tau(2)\ \tau(3))\cdot\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}$$

で，したがって，

$$(\tau(2)\ \tau(3))(\sigma(1)\ \sigma(2))\cdot\sigma=\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix},$$

$$\sigma=(\sigma(1)\ \sigma(2))^{-1}\ (\tau(2)\ \tau(3))^{-1}=(\sigma(1)\ \sigma(2))(\tau(2)\ \tau(3))$$

となる．このようにσの偶奇は転位の個数の偶奇と一致する．

具体的なσが偶置換であるか奇置換であるかを見分けるには，このように転位の個数を調べるのが簡単である．

S_nの元σの符号を

$$\mathrm{sgn}\ \sigma=\begin{cases}\ \ 1 & (\sigma\ \text{が偶置換のとき})\\ -1 & (\sigma\ \text{が奇置換のとき})\end{cases},$$

ときめる．

補題 1.28　1と-1とからなる乗法群をGとおく(1.1節例5)．S_nからGへの写像fを

$$f: S_n\to G,\quad \sigma\to\mathrm{sgn}\ \sigma$$

ときめる．S_nの2元σ,τに対して

$$\mathrm{sgn}\ \sigma\tau=\mathrm{sgn}\ \sigma\cdot\mathrm{sgn}\ \tau$$

が成り立って，fは全射準同型である．

補題1.28のfの核

$$\mathrm{Ker}\ f=\{\sigma\in S_n\mid \sigma\ \text{は偶置換}\}$$

はS_nの正規部分群で，これをA_nであらわし，n次の**交代群**とよぶ．

$$S_n/A_n\cong G=\{1,-1\}$$

であるから，剰余群S_n/A_nの位数は2．したがって，

$$|A_n|=|S_n|/(S_n:A_n)=\frac{n!}{2}$$

となる(定理1.10)．

例 4　n次$(n>2)$の交代群A_nは$(n-2)$個の3次の巡回置換$(1\ 2\ 3)$, $(1\ 2\ 4),\cdots,(1\ 2\ n)$から生成される．

実際，定理1.26からA_nの各元は$(1\ k)\ (k\neq 1)$の形の互換の偶数個の積としてあらわされる．このとき，恒等写像$(1\ 2)(1\ 2)$をはさんで

$$(1\ k)(1\ k')=(1\ k)(1\ 2)\cdot(1\ 2)(1\ k')$$

と変形する．$k\neq 2$ならば，

$$(1\ k)(1\ 2)=(1\ 2\ k),\quad (1\ 2)(1\ k)=(1\ 2\ k)^{-1}.$$

$k=2$のときは$(1\ k)(1\ 2),(1\ 2)(1\ k)$共に恒等写像で，これを除いてもかまわない．したがって，$(1\ 2\ k)\ (3\leqq k\leqq n)$から生成される．

例 5 A_n $(n \geqq 5)$ は単純群である．

HをA_nの正規部分群 $(\neq \{e\})$ とし，$H=A_n$を示す．Hに属する置換の中で動くXの元の数が最小であるものをσとする．まず，σが3個のXの元のみを動かす，すなわち，3次の巡回置換であることを示す．そのために，σが少なくとも4個のXの元を動かすと仮定する．

σを共通なXの元を含まない巡回置換の積に分解すると，σは互換ばかりの積か，そうでなければ3以上の次数の巡回置換を含む．したがって，σが

(1)　$(1\ \ 2)(3\ \ 4)\cdots$

の形をしているか，または

(2)　$(1\ \ 2\ \ 3\ \cdots)\cdots$

の形をしていると考えてよい．(2)の形のσがちょうど4個のXの元を動かすならば，σは4次の巡回置換で奇置換となって矛盾である．(2)の形のσは1, 2, 3, 4, 5を実際に動かすとしてよい．

$\tau=(3\ \ 4\ \ 5)$ とおく．

(1)のσに対して $\tau\sigma\tau^{-1}=(1\ \ 2)(4\ \ 5)\cdots$,

(2)のσに対して $\tau\sigma\tau^{-1}=(1\ \ 2\ \ 4\ \cdots)\cdots$.

(1), (2) いずれの形のσに対しても $\tau\sigma\tau^{-1}\neq\sigma$ で，$\sigma^{-1}(\tau\sigma\tau^{-1})=\sigma'$ とかけばσ'はeと異なるHの元である．Xの元k (>5) がσで動かないならば，kはτで動かないからσ'でも動かない．また，(1)の形のσに対してはσ'は1も2も動かさないから，σ'で動くXの元の数はσのそれより少なく矛盾である．(2)の形のσに対してはσ'は1を動かさないから，σ'で動くXの元の数はこのときもσのそれより少なく矛盾である．

したがって，σは3個のみのXの元を動かし，それを$\sigma=(1\ \ 2\ \ 3)$としてよい．i $(\geqq 3)$ がXの元ならば，S_nの中に

$$\begin{pmatrix} 1 & 2 & 3 & \cdots \\ 1 & 2 & i & \cdots \end{pmatrix}$$

という置換がある．これをρとかく．ρが奇置換ならば$n-1\geqq 4$であるから

$$\begin{pmatrix} 1 & 2 & 3 & \cdots \\ 1 & 2 & i & \cdots \end{pmatrix}\cdot(n-1\ \ n)$$

もS_nに属する．これを改めてρとかき，ρを偶置換と考える．このとき

$$\rho\sigma\rho^{-1}=(1\ \ 2\ \ i)$$

はHに属する．したがって，例4から$A_n=H$となる．

例 6 n次正方行列$A=(a_{ij})$の行列式を

$$\sum \operatorname{sgn}\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \cdot a_{1i_1}a_{2i_2}\cdots a_{ni_n}$$

と定義し，$|A|$ であらわした．ここで $\sum$ は，$\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$ が n 次の対称群 S_n のすべての元をわたるときの $n!$ 個の和をあらわす．

例えば，$A=\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ に対しては $S_2=\left\{\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\right\}$ であるから

$$|A|=\operatorname{sgn}\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}\cdot a_{11}a_{22}+\operatorname{sgn}\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\cdot a_{12}a_{21}=a_{11}a_{22}-a_{12}a_{21}$$

であり，$A=\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$ に対しては，1.1 節例 6 から

$$\begin{aligned} |A| &= a_{11}a_{22}a_{33}+a_{12}a_{23}a_{31}+a_{13}a_{21}a_{32} \\ &\quad -a_{11}a_{23}a_{32}-a_{13}a_{22}a_{31}-a_{12}a_{21}a_{33} \end{aligned}$$

である．行列式 $|A|$ を与えるこの 2 つの式を**サルスの規則**とよんでいる．

演習問題 1

1.　定理 1.1 を証明せよ．

2.　定理 1.3 は有限集合でないとかならずしも成り立たないことを示せ．

3.　群 G の任意の元 a に対して $a^2=e$（e は G の単位元）が成り立つならば，G はアーベル群であることを示せ．

4.　2 次の対称群 S_2 が位数 2 のアーベル群であることを示し，乗積表をつくれ．

5.　$G=\{(a,b)\in \boldsymbol{R}\times\boldsymbol{R} \mid a\neq 0\}$ とおく．G の 2 元 $(a,b), (a',b')$ の積を

$$(a,b)\cdot(a',b')=(aa', ba'+b')$$

ときめると，G は群をつくることを示せ．また，G はアーベル群でないことを示せ．

6.　集合 S の部分集合の全体を G とする．G の 2 元 A, B の積を

$$AB=A\cup B-A\cap B$$

ときめると，G はアーベル群をつくることを示せ．

7.　$H=\{z=\alpha+\beta i\in\boldsymbol{C} \mid \alpha, \beta\in\boldsymbol{R}, \beta>0\}$ とおく．$a, b, c, d\in\boldsymbol{Z}, ad-bc=1$ として写像 f を

$$f: H \to H, \quad z \to \frac{az+b}{cz+d}$$

ときめる．fをモジュラー変換とよぶ．このとき次のことを示せ．

(1) $z \in H$ならば，$f(z) \in H$.

(2) モジュラー変換の全体は写像の合成を演算として群をつくる．この群を**モジュラー変換群**とよぶ．

8. 平面上に直交軸が与えられているとき，平面上の点のx軸，y軸，原点に関する対称移動は，恒等写像とあわせて位数4のアーベル群をつくることを示せ．また，乗積表をつくれ．

9. 平面αの運動でαの上の正方形をそれ自身に重ねるものの全体は，写像の合成を演算として群をつくることを示せ．この群を4次の**二面体群**とよぶ．

10. Gを群，aをGの元とする．任意の整数m, nに対して$(a^m)^n = a^{mn}$が成り立つことを示せ．

11. 群Gの元$a_1, a_2, \cdots, a_n$ $(n \geqq 3)$に対して，$1 \leqq i \leqq n-1$ならば，

$$(a_1 a_2 \cdots a_i) \cdot (a_{i+1} \cdots a_n) = a_1 a_2 \cdots a_n$$

であることを示せ．

12. 群Gが部分集合Sから生成された有限群ならば，Gの任意の元はSの元の積の形であらわされることを示せ．

13. 群Gの部分集合HがGの演算で群をつくるならば，HはGの部分群であることを示せ．

14. Hが群Gの部分群，KがHの部分群ならば，KはGの部分群であることを示せ．

15. (1) 3次の二面体群の部分群をすべてかきあげよ．

(2) 4次の二面体群の部分群をすべてかきあげよ．

16. 群Gの空でない部分集合S, S'に対して，次のことを示せ．

(1) SがGの部分群ならば，$SS=S, S^{-1}=S$が成り立つ．

(2) S, S'が共にGの部分群のとき

$$SS' \text{が} G \text{の部分群} \Leftrightarrow SS'=S'S.$$

17. $K_1, K_2, \cdots$が群Gの部分群Hを法とする左剰余類であって，$G = \cup K_i$であるならば，$G = \cup K_i^{-1}$でもあることを示せ．

18. $X = \{1, 2, \cdots, n\}$とおく．n次の対称群S_nの元でnを動かさないものの全体をHとおく．このとき，次のことを示せ．

(1) HはS_nの部分群である．

(2) S_nの元a, bがHを法として左合同 $\Leftrightarrow$ $a(n)=b(n)$.
ここで$a(n)$はnのaによる像をあらわす.

(3) $1\leqq i\leqq n$に対して，iをnに，nをiにうつしてi, n以外のXの元を動かさないS_nの元をa_iとかけば，$a_1, a_2, \cdots, a_n$のどの2つもHを法として左合同ではない.

(4) $a_1, a_2, \cdots, a_n$はS_nのHを法とする1つの完全代表系である.

(5) Hを$(n-1)$次の対称群S_{n-1}とみなせば，$|S_n|=n\cdot|S_{n-1}|$が成り立つ.

19. Gが群，Kが部分群，Hが正規部分群のとき，次のことを示せ.

(1) $HK=KH$.

(2) HKはGの部分群で$H\lhd HK$.

(3) $H\cap K\lhd K$.

20. N_1, N_2が群Gの正規部分群ならば，$N_1N_2, N_1\cap N_2$もまたGの正規部分群であることを示せ.

21. Gが群，H, KはGの部分群で$K\subseteqq H$とする．このとき

① KはHの部分群である,

② $(G:H), (H:K)$が共に有限 $\Leftrightarrow$ $(G:K)$が有限

ならば，$(G:K)=(G:H)\cdot(H:K)$であることを示せ.

22. 群Gの空でない部分集合Sに対して

$$N(S)=\{a\in G \mid aS=Sa\}$$

ときめる．このとき，次のことを示せ.

(1) $N(S)$はGの部分群をつくる．これをSのGにおける**正規化群**とよぶ.

(2) SがGの部分群ならば，$N(S)$はSを含み，Sは$N(S)$の正規部分群である.

(3) SがGの部分群ならば，$N(S)$はSを正規部分群として含むGの最大の部分群である.

23. 定理1.17の(1), (4)を証明せよ.

24. 乗法群$\boldsymbol{C}^*$から1次元のトーラス群Tへの写像fを

$$f: \boldsymbol{C}^* \to T, \quad z \to \frac{z}{|z|}$$

ときめる．fは一意写像であり，全射準同型で，$\operatorname{Ker} f=\boldsymbol{R}^+$であることを示せ.

25. 群GからGへの同型写像をGの**自己同型**とよぶ．次のことを示せ.

(1) Gの自己同型の全体$A(G)$は，Gの上の対称群の部分群をつくる.

(2)　Gの内部自己同型の全体 $I(G)$ は $A(G)$ の正規部分群をつくる．

(3)　Gの中心 $Z(G)$ はGの正規部分群で，$I(G)$ は $G/Z(G)$ に同型である．

26.　写像 $f: \boldsymbol{Z}\to\boldsymbol{Z}$ を加法群 $\boldsymbol{Z}$ の準同型とする．

(1)　fが単射 $\Leftrightarrow$ $f(1)\neq 0$ であることを示せ．

(2)　fが全射 $\Leftrightarrow$ $f(1)=\pm 1$ であることを示せ．

(3)　$A(\boldsymbol{Z})$ を求めよ．

27.　(1)　写像 $f: \boldsymbol{Q}\to\boldsymbol{Q}$ が加法群 $\boldsymbol{Q}$ の準同型ならば，$\dfrac{b}{a}\in\boldsymbol{Q}$ に対して $f\left(\dfrac{b}{a}\right)=\dfrac{b}{a}\cdot f(1)$ を示せ．

(2)　fに$f(1)$ を対応させて $A(\boldsymbol{Q})$ と $\boldsymbol{Q}^*$ とが同型であることを示せ．

28.　任意の群Gは適当な集合Xの上の対称群の部分群と同型であることを示せ．

29.　G, G' を群，$f: G\to G'$ を全射準同型とする．このとき，G' の正規部分群 H' に対して

$$G/f^{-1}(H')\cong G'/H'$$

であることを示せ．これを**第一同型定理**とよぶことがある．

30.　Gを群，HをGの正規部分群とする．Gの任意の部分群Kに対して

$$K/K\cap H\cong KH/H$$

であることを示せ．これを**第二同型定理**とよぶことがある．

31.　Gを群，aをGの元とする．Gにおけるaの正規化群 $N(a)=\{x\in G\mid ax=xa\}$ に対して，次のことを示せ．

(1)　x, y をGの元とすれば，

$$xax^{-1}=yay^{-1} \Leftrightarrow x^{-1}y\in N(a).$$

(2)　Gが有限群ならば，aの共役類に含まれる相異なる元の個数は $(G:N(a))$ に等しい．

32.　Hを群Gの部分群とする．次のことを示せ．

(1)　Gの元aに対して，aHa^{-1} はGの部分群である．この形の部分群をHの**共役部分群**とよぶ．

(2)　Hの共役部分群全部の共通部分 $\bigcap_{a\in G} aHa^{-1}$ はGの正規部分群である．

(3)　$\bigcap_{a\in G} aHa^{-1}$ はHに含まれるGの正規部分群の中で最大である．

33.　整数 $a_1, a_2, \cdots, a_n$ の中に0でないものがあるとき，次のことを示せ．

dが $a_1, a_2, \cdots, a_n$ の最大公約数

$\Leftrightarrow$ (1)　dは $a_1, a_2, \cdots, a_n$ の正の公約数．

(2)　$a_1, a_2, \cdots, a_n$ の任意の公約数は d を割り切る.

34.　整数 $a_1, a_2, \cdots, a_n$ のすべてが 0 でないとき，次のことを示せ.

l が $a_1, a_2, \cdots, a_n$ の最小公倍数

$\Leftrightarrow$ (1)　l は $a_1, a_2, \cdots, a_n$ の正の公倍数.

(2)　l は $a_1, a_2, \cdots, a_n$ の任意の公倍数を割り切る.

35.　整数 a, b, 自然数 m に対して，m を法として a, b が合同ならば，a と m, b と m の最大公約数は一致することを示せ.

36.　$G=(a)$ が位数 m の巡回群で，$m=st$ $(s>0)$ とかけば,

$$(a^s)=\{x\in G \mid x^t=e\}$$

であることを示せ.

37.　乗法群 $\boldsymbol{Q}^*$ では位数有限の元は ± 1 にかぎられることを示せ.

38.　a, b が群 G の元で ab の位数が有限ならば，ba の位数も有限で 2 つの位数は一致することを示せ.

39.　a, b が群 G の元で $ab=ba$ とする．a の位数を m, b の位数を n とおく．このとき，次のことを示せ.

(1)　m, n が互いに素 $\Leftrightarrow$ ab の位数 $=mn$.

(2)　$n|m$ $\Leftrightarrow$ $(a)\cdot(b)$ の元の位数は m をこえない.

40.　m, n が互いに素な自然数ならば，1 の原始 m 乗根と 1 の原始 n 乗根との積は 1 の原始 mn 乗根であることを示せ.

41.　群 G の元 a, 整数 $n\neq 0$ に対して，次のことを示せ.

(1)　a の位数が無限ならば，a^n の位数も無限である.

(2)　a の位数が m ならば，a^n の位数は $\dfrac{m}{(m, n)}$ である.

42.　アーベル群の位数有限の元の全体は部分群をつくることを示せ.

43.　巡回群 G, G' に対して，次のことを示せ.

(1)　G, G' が共に無限群 $\Rightarrow$ $G\cong G'$.

(2)　G, G' が共に有限群のときは

$|G'|\,\big|\,|G|$ $\Leftrightarrow$ G から G' への全射準同型がある.

$|G|=|G'|$ $\Leftrightarrow$ $G\cong G'$.

44.　G を位数 m の有限群，H を位数 s の G の正規部分群とする．$m=st$ とかいたとき，s, t が互いに素ならば

$$H=\{x\in G \mid x^s=e\}$$

であることを示せ.

45.　Gを位数mの巡回群，sをmの正の約数とする．このとき，次のことを示せ．

(1)　Gの元で位数sのものは$\varphi(s)$個存在する．

(2)　$\sum_{s|m}\varphi(s)=m$.

ここで(2)の左辺の和は，mのすべての正の約数sの上をわたるものとする．

46.　G, G'を群とし，GとG'の直積$G\times G'$の2元(a, a'), (b, b')の積を

$$(a, a')\cdot(b, b')=(ab, a'b')$$

ときめると，$G\times G'$は群をつくることを示せ．これをG, G'の**直積**とよぶ．また，G, G'が位数m, m'の巡回群のとき，

$$m, m' \text{が互いに素} \Leftrightarrow G\times G' \text{が巡回群}$$

であることを示せ．

47.　Gを群，H, KをGの部分群とする．もし

①　$a\in H, b\in K \Rightarrow ab=ba$,

②　Gの元は$ab\ (a\in H, b\in K)$の形に一意的にあらわされる

ならば，GはH, Kの**直積に分解される**という．このとき，次のことを示せ．

(1)　GがH, Kの直積に分解される $\Rightarrow G\cong H\times K$.

(2)　GがH, Kの直積に分解される

$\Leftrightarrow H, K\lhd G$ で $G=HK,\ H\cap K=\{e\}$.

(3)　GがH, Kの直積に分解される $\Rightarrow G/H\cong K, G/K\cong H$.

48.　乗法群$\boldsymbol{R}^*$は正の実数の乗法群$\boldsymbol{R}^+$と乗法群$\{1, -1\}$の直積に分解されることを示せ．

49.　乗法群$\boldsymbol{C}^*$は$\boldsymbol{R}^+$とトーラス群Tの直積に分解されることを示せ．

50.　pを素数，Gを位数p^2の群とする．Gは巡回群かまたは位数pの2個の巡回部分群の直積に分解されることを示せ．

51.　S_5において$\begin{pmatrix}1&2&3&4&5\\4&5&3&2&1\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\5&3&4&2&1\end{pmatrix}^{-1}(1\ \ 2)(1\ \ 3\ \ 2\ \ 4)^{-1}$

$\times(2\ \ 5\ \ 4\ \ 3)$を求めよ．

52.　S_nにおいて，次のことを示せ．

(1)　$(i_1\,i_2\cdots i_s)=(i_1\,i_s)(i_1\,i_{s-1})\cdots(i_1\,i_2)$.

(2)　$(i_1\,i_2)^{-1}=(i_1\,i_2)$.

(3)　$\begin{pmatrix}1&2&\cdots&n\\i_1&i_2&\cdots&i_n\end{pmatrix}\begin{pmatrix}1&2&\cdots&n\\j_1&j_2&\cdots&j_n\end{pmatrix}\begin{pmatrix}1&2&\cdots&n\\i_1&i_2&\cdots&i_n\end{pmatrix}^{-1}=\begin{pmatrix}i_1&i_2&\cdots&i_n\\i_{j_1}&i_{j_2}&\cdots&i_{j_n}\end{pmatrix}$.

53.　共通なXの元を含まない巡回置換の積は交換可能であることを示せ．

54. S_n の元 $\sigma=\begin{pmatrix}1 & 2 & \cdots & n-1 & n\\ 2 & 3 & \cdots & n & 1\end{pmatrix}$ に対して $e, \sigma, \sigma^2, \cdots, \sigma^{n-1}$ は位数 n の巡回群をつくることを示せ.

55. $S_n\ (n\geqq 2)$ は $(1\ 2), (1\ 3), \cdots, (1\ n)$ の $(n-1)$ 個の互換で生成されることを示せ.

56. S_3 において，次のものを求めよ.

(1) すべての共役類.

(2) $a=(1\ 2), (1\ 2\ 3)$ として $N(a), (S_3:N(a))$.

(3) 類等式.

57. $S_n\ (n\geqq 3)$ のすべての 3 次の巡回置換によって生成される部分群は A_n であることを示せ.

58. S_n の元 σ によって動かされる最小の X の元を i とし，σ が i を j にうつすとすると，$(j-1\ \ j)\sigma$ の転位の個数は σ の転位の個数より 1 だけ少ないことを示せ.

59. S_n の元 σ が s 個の転位をもつならば，$(i\ \ i+1)$ の形の互換の s 個の積としてあらわされることを示せ.

60. S_n から乗法群 $\boldsymbol{C}^*$ への準同型 f は

① 任意の $\sigma\in S_n$ に対して $f(\sigma)=1$,

② 任意の $\sigma\in S_n$ に対して $f(\sigma)=\mathrm{sgn}\,\sigma$

のいずれかにかぎられることを示せ.

2

環

$\boldsymbol{Z}$は加法と乗法の2つの演算をもった集合で環とよばれている．$\boldsymbol{Q}, \boldsymbol{R}, \boldsymbol{C}$も環であり．環の元を成分とする正方行列の全体，環の元を係数とする多項式の全体等も環をつくる．環は2つの演算をもつ意味で，群とは本質的に異なった構造をもつ．この章では環のもついろいろな性質についてのべる．

2.1 環の定義

空でない集合Rの上に2つの演算φ_1, φ_2: $R\times R\to R$があって

1. φ_1に関してRはアーベル群をつくる，
2. φ_2に関してRは結合法則をみたす，
3. Rの任意の元a, b, cに対して，φ_1とφ_2の間には

$$\varphi_2(a, \varphi_1(b, c))=\varphi_1(\varphi_2(a, b), \varphi_2(a, c)),$$
$$\varphi_2(\varphi_1(a, b), c)=\varphi_1(\varphi_2(a, c), \varphi_2(b, c))$$

が成り立つ，

4. φ_2に関してRは単位元をもつ

の4つの公理をみたすとき，Rを**環**とよぶ．

普通φ_1をRの**加法**とよび，$\varphi_1(a, b)=a+b$とかく．$a+b$をRの元a, bの**和**とよぶ．φ_2をRの**乗法**とよび，$\varphi_2(a, b)=a\cdot b$またはabであらわす．abをRの元a, bの**積**とよぶ．

加法，乗法の記号を用いれば，環の4つの公理は

1. Rは加法群である，
2. Rの任意の元a, b, cに対して

$$(ab)c=a(bc)$$

が成り立つ，

3. Rの任意の元a,b,cに対して

$$a\cdot(b+c)=ab+ac, \quad (a+b)\cdot c=ac+bc$$

が成り立つ，

4. Rに元eがあって，Rの任意の元aに対して

$$a\cdot e=e\cdot a=a$$

が成り立つ

となる．

公理3の2つの等式はRの加法と乗法を結ぶ関係式で，これを**分配法則**とよんでいる．

環Rは加法群である．この群の単位元をRの**零元**とよび，0であらわす．Rの乗法に関する単位元eを普通1であらわし，単にRの**単位元**という．Rの零元がただ1個しかないことは1.1節でのべたが，Rの単位元もただ1個であることを同じようにして証明できる．

特に，Rの任意の元a,bに対して

$$a\cdot b=b\cdot a$$

が成り立つような環Rを**可換環**とよぶ．

例 1　$\boldsymbol{Z}$は数の加法，乗法に関して可換環をつくる．数の0が$\boldsymbol{Z}$の零元であり，数の1が$\boldsymbol{Z}$の単位元である．この環$\boldsymbol{Z}$を(有理)**整数環**とよぶ．同じように$\boldsymbol{Q},\boldsymbol{R},\boldsymbol{C}$も可換環である．

例 2　実数を成分とする2×2行列の全体も行列の加法，乗法に関して環をつくる．零行列$\begin{pmatrix}0&0\\0&0\end{pmatrix}$がこの環の零元であり，単位行列$\begin{pmatrix}1&0\\0&1\end{pmatrix}$が単位元である．この環を$\boldsymbol{R}$の上の2次の**行列環**とよび，$(\boldsymbol{R})_2$であらわす．

$$\begin{pmatrix}1&0\\0&0\end{pmatrix}\cdot\begin{pmatrix}0&1\\0&0\end{pmatrix}=\begin{pmatrix}0&1\\0&0\end{pmatrix}, \quad \begin{pmatrix}0&1\\0&0\end{pmatrix}\cdot\begin{pmatrix}1&0\\0&0\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$$

であるから，$(\boldsymbol{R})_2$は可換環ではない．

実数を係数とする多項式の全体もまた環をつくる．この環については2.5節で詳しくのべる．

例 3　Xを空でない集合とし，Xから$\boldsymbol{R}$への写像の全体をRとおく．2つの写像$f,g\colon X\to\boldsymbol{R}$の和と積を

$$f+g\colon X \to \boldsymbol{R}, \quad x \to f(x)+g(x)$$

$$f\cdot g\colon X \to \boldsymbol{R},\quad x \to f(x)g(x)$$

ときめると，Rに加法と乗法が定義できてRは可換環をつくる．

例えば，Rが加法に関して結合法則をみたすことは，$f, g, h \in R$, $x \in X$ に対して

$$((f+g)+h)(x)=(f+g)(x)+h(x)=(f(x)+g(x))+h(x),$$
$$(f+(g+h))(x)=f(x)+(g+h)(x)=f(x)+(g(x)+h(x))$$

であり，$\boldsymbol{R}$ が加法に関して結合法則をみたすから

$$(f(x)+g(x))+h(x)=f(x)+(g(x)+h(x))$$

で，$(f+g)+h=f+(g+h)$ をうる．

すべてのXの元を実数0にうつす写像がRの零元である．Rの元fの加法に関する逆元 $-f$ は,

$$-f\colon X \to \boldsymbol{R},\quad x \to -f(x)$$

ときめればよい．

Rが乗法に関する結合法則と分配法則をみたすことも同じように確かめられる．すべてのXの元を実数1にうつす写像がRの単位元となる．

Xとして $\boldsymbol{R}$ をとり，$\boldsymbol{R}$ から $\boldsymbol{R}$ への特別な写像(例えば連続な写像)の全体も同じようにして可換環をつくる．

例 4 Mを加法群とし，MからMへの準同型(このような準同型をMの**自己準同型**とよぶ)の全体をRとかく．Rの2元f, gの和と積を

$$f+g\colon M \to M,\quad x \to f(x)+g(x),$$
$$f\cdot g\colon M \to M,\quad x \to f(g(x))$$

ときめると，Rに加法と乗法が定義できてRは環となる．

例えば，$f\cdot g$ が準同型であることは，Mの元x, yに対して

$$(f\cdot g)(x+y)=f(g(x+y))=f(g(x)+g(y))$$
$$=f(g(x))+f(g(y))=(f\cdot g)(x)+(f\cdot g)(y)$$

であることから分かる．

Rの零元はMのすべての元をMの零元にうつす写像であり，Rの単位元はMの恒等写像である．この環RをMの**自己準同型環**とよび，End (M) とかく．

補題 2.1 Rを環，a, bをRの元とすると

(1) $a\cdot 0=0\cdot a=0.$

(2) $a\cdot(-b)=(-a)\cdot b=-ab.$

(3)　$(-a)\cdot(-b)=ab$.

証明　(1)　分配法則を用いて

$$a\cdot 0=a\cdot(0+0)=a\cdot 0+a\cdot 0$$

から $a\cdot 0=0$ をうる．$0\cdot a=0$ も同じように証明できる．

(2)
$$a\cdot(-b)+ab=a\cdot(-b+b)=a\cdot 0=0$$

であるから，$a\cdot(-b)=-ab$ である．$(-a)\cdot b=-ab$ も同じように証明できる．

(3)の証明は演習問題とする．

環 R は単位元1と零元0をもつ．もし $1=0$ ならば，R の任意の元 a に対して，補題2.1から

$$a=a\cdot 1=a\cdot 0=0$$

で，$R=\{0\}$ となる．このような R を**零環**とよぶ．普通，環というときは零環でない環を問題とするので，以下 $1\neq 0$ と約束する．

例2の行列環 $(\boldsymbol{R})_2$ では，$\begin{pmatrix}1&0\\0&0\end{pmatrix}$ も $\begin{pmatrix}0&0\\0&1\end{pmatrix}$ も零元ではないが，その積は

$$\begin{pmatrix}1&0\\0&0\end{pmatrix}\cdot\begin{pmatrix}0&0\\0&1\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$$

のように零元となる．一般に，環 R の元 $a\neq 0$ に対して R の元 $b\neq 0$ があって $a\cdot b=0$ であるとき，a を R の**左零因子**とよぶ．右零因子も同じように定義できる．可換環 R では左右の区別はいらない．

零因子をもたない可換環を**整域**とよぶ．可換環 R に対しては

$$R\text{が整域} \Leftrightarrow (a,b\in R \text{ で } a\neq 0, b\neq 0 \Rightarrow ab\neq 0)$$

が成り立つ．

例 5　$\boldsymbol{Z}$ は整域である．$\boldsymbol{Q}, \boldsymbol{R}, \boldsymbol{C}$ も整域である．

環 R の元 a に対して

$$a\cdot b=b\cdot a=1$$

となる R の元 b が存在するとき，a を R の**単元**，b を a の**逆元**という．a の逆元 b は，1.1節で示したように，a に対してただ1個きまり，これを a^{-1} とかく．

例 6　$\boldsymbol{Z}$ では ± 1 のみが単元であり，$(\boldsymbol{R})_2$ では $\begin{pmatrix}a&b\\c&d\end{pmatrix}$ が単元とは $ad-bc$

$\neq 0$ を意味する．このような行列を正則な行列とよんだ (1.1 節例 4)．この行列の逆行列は $\dfrac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ で与えられる．

環 R の 0 でない元がすべて単元であるとき，R を**斜体**とよぶ．R が可換環で斜体であるとき，R を**体**とよぶ．

例 7 $\boldsymbol{Q}, \boldsymbol{R}, \boldsymbol{C}$ はすべて体で，それぞれを**有理数体**，**実数体**，**複素数体**とよんでいる．

例 8 体は整域であるが，有限個の元からなる整域は体である．

体 R が整域であることは，$a, b \in R$ $(a \neq 0)$ で $ab=0$ ならば $b=(a^{-1}a)b=a^{-1}\cdot(ab)=0$ であることから分かる．後半を証明するために，R が有限個の元からなる整域で，$a \in R$ $(a \neq 0)$ とする．写像 f を

$$f\colon R \to R, \quad x \to ax$$

ときめれば，f は一意写像であり R が零因子をもたないから，f は単射である．R は有限集合，したがって，f は全射で

$$R=f(R)=\{ax \mid x \in R\}.$$

R の単位元 1 に対して $ax=1$ をみたす R の元 x が存在する．したがって，a は R の単元である．

例 9 複素数を成分とする 2×2 行列

$$E=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I=\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad J=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad K=\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

に対して

$$R=\{aE+bI+cJ+dK \mid a, b, c, d \in \boldsymbol{R}\}$$

とおく．R は行列の加法，乗法に関して非可換な斜体をつくる．この R を**4元数環**とよぶ．R の元

$$aE+bI+cJ+dK=\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$$

に対して，$(a+bi)\cdot(a-bi)-(c+di)\cdot(-c+di)=a^2+b^2+c^2+d^2$ から

$$aE+bI+cJ+dK \text{ が単元} \Leftrightarrow a, b, c, d \text{ いずれかが } 0 \text{ でない}$$

であることが分かる．詳しい証明は演習問題とする．

群に対して部分群を考えたと同じように，環に対して部分環が考えられる．環 R の部分集合 S が，R の単位元 1 を含み，R の加法，乗法に関して環をつく

るとき，SをRの**部分環**とよぶ．

補題 2.2　Rを環，SをRの空でない部分集合とする．このとき

SがRの部分環 $\Leftrightarrow$ (1)　SはRの単位元 1 を含む，

(2)　$a, b\in S \Rightarrow a-b, ab\in S$.

証明　$\Rightarrow$: (1) は明らかであるから (2) を示す．SがRの部分環ならば，SはRの加法に関して群をつくる．したがって，Sは加法群Rの部分群で，$a, b\in S$ならば$a-b\in S$である(定理 1.5)．また，SがRの部分環ならば，Rの乗法をSに制限してSの乗法がえられるから，$a, b\in S$ならば$ab\in S$でなければならない．

$\Leftarrow$: まず，(1), (2) から $0=1-1\in S$ である．また，(2) から $a, b\in S$ ならば $-b=0+(-b)=0-b\in S$ で，したがって，

$$a+b=a-(-b)\in S$$

となる．$ab\in S$ とあわせて，Rの演算をSに制限してSは加法，乗法の 2 つの演算をもつ．

定理 1.5 からSは加法に関してRの部分群をつくり，Sは環の公理 1 をみたす．環の公理 2, 3 はRがみたしているから，Sも自然にみたす．Rの単位元はSにとっても単位元であり，環の公理 4 も成り立つ．したがって，Sは環をつくる．

例 10　$\boldsymbol{Z}$は$\boldsymbol{Q}$の部分環であり，$\boldsymbol{Q}$は$\boldsymbol{R}$の，$\boldsymbol{R}$は$\boldsymbol{C}$の部分環である．$\boldsymbol{C}$の部分集合

$$\{a+bi\in\boldsymbol{C}\mid a, b\in\boldsymbol{Z}\}$$

は$\boldsymbol{C}$の部分環をつくる．この部分環を**ガウスの整数環**とよび，$\boldsymbol{Z}[i]$ であらわす．

例 11　行列環 $(\boldsymbol{R})_2$ の部分集合

$$\left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\middle|\ a, b, c\in\boldsymbol{R}\right\}$$

は $(\boldsymbol{R})_2$ の部分環をつくる．この部分環を $\boldsymbol{R}$ の上の**三角行列環**とよぶ．

可換環Rの部分環Sが体をなすとき，SをRの**部分体**とよぶ．

補題 2.3　Rが体ならば，Rの空でも $\{0\}$ でもない部分集合Sに対して

SがRの部分体 $\Leftrightarrow$ (1)　$a, b\in S \Rightarrow a-b\in S$,

(2)　$a, b\in S, b\neq 0 \Rightarrow ab^{-1}\in S$.

証明　$\Rightarrow$: SはRの部分環であるから (1) は明らか．(2) を示すために，a, b

$\in S, b \neq 0$ とする．Sは体をつくるから，bはSの単元で$bb'=1$をみたすSの元b'が存在する．Rにおけるbの逆元b^{-1}をかけて$b'=b^{-1}$をうるから$b^{-1} \in S$．補題2.2を用いて$ab^{-1} \in S$となる．

$\Leftarrow$: Sは空でも$\{0\}$でもないから，Sの中に0でない元cがある．(1)から$0=c-c \in S$であり，(2)から$1=cc^{-1} \in S$である．

$a, b \in S$ならば$ab \in S$を示す．$b=0$のときは$ab=0 \in S$である．$b \neq 0$のときは，(2)で$a=1$にとって$b^{-1}=ab^{-1} \in S$が分かる．a, b^{-1}に(2)を適用して，$ab=a(b^{-1})^{-1} \in S$となる．(1)とあわせて補題2.2から，SはRの部分環である．

$S \ni b \neq 0$ならば$b^{-1} \in S$を示したが，これはSが体であることを意味している．

例 12 $\boldsymbol{Q}$は$\boldsymbol{R}$の部分体であり，$\boldsymbol{R}$は$\boldsymbol{C}$の部分体である．

2.2 イデアルと剰余環

環Rの空でない部分集合Aで

(1) $a, b \in A \Rightarrow a+b \in A$,

(2) $a \in A,\ c \in R \Rightarrow ca \in A$

の2つの条件をみたすものをRの**左イデアル**とよぶ．

AがRの左イデアルならば，$a, b \in A$であるとき

$$-b=(-1)\cdot b \in A \text{ で } a-b=a+(-b) \in A$$

であるから

(1)′ $a, b \in A \Rightarrow a-b \in A$

をみたす．また，$a+b=a-(-b)$であるから，左イデアルの定義で(1)を(1)′におきかえてもよい．Rの左イデアルは加法群Rの部分群でもある．

Rの**右イデアル**も同じように定義できる．AがRの左イデアルであり，同時にRの右イデアルでもあるとき，Aを単にRの**イデアル**とよぶ．Rが可換環のときは左右の区別はいらない．

R自身も，Rの零元のみからなる集合$\{0\}$も共にRのイデアルである．この2つのイデアルを**自明なイデアル**とよぶ．

Rの左イデアルAがRの単位元1を含めば，(2)からRの元をすべて含み，したがって，$A=R$で，Aは自明なイデアルとなる．

例 1 $\boldsymbol{Z}$の(左)イデアルは，上に注意したように，加法群$\boldsymbol{Z}$の部分群である．逆に，加法群$\boldsymbol{Z}$の部分群は(左)イデアルの条件(1), (2)を常にみたす．し

たがって，$\boldsymbol{Z}$ ではイデアルと加法群 $\boldsymbol{Z}$ の部分群とは全く同じ概念である．

例 2　環 R の元 a に対して

$$A=\{xa \mid x\in R\}$$

は a を含む R の左イデアルで，しかも，そのような R の左イデアルの中で最も小さい．この A を a から**生成**された R の左イデアルとよび

$$A=Ra \quad \text{または} \quad A=(a)$$

であらわす．このようにただ1個の元から生成された左イデアルを**単項左イデアル**とよぶ．**単項右イデアル**も同じように定義できる．R が可換のときは，左右の区別はいらない．単に**単項イデアル**とよぶ．

1.2節例10によれば，$\boldsymbol{Z}$ の $\{0\}$ でないイデアルはある自然数 m から生成された単項イデアル $(m)=\{xm \mid x\in\boldsymbol{Z}\}$ でつくされる．$\boldsymbol{Z}$ の0のみからなるイデアルも0から生成された単項イデアルであるから，$\boldsymbol{Z}$ のイデアルはすべて単項イデアルである．

$\boldsymbol{Z}$ のように，整域であって，そのイデアルがすべて単項イデアルであるものを**単項イデアル整域**という．

例 3　環 R の左イデアル $A_1, A_2, \cdots, A_n$ に対して，その**和**を

$$\{b_1+b_2+\cdots+b_n \mid b_1\in A_1, b_2\in A_2, \cdots, b_n\in A_n\}$$

ときめ，

$$A_1+A_2+\cdots+A_n$$

であらわす．$A_1+A_2+\cdots+A_n$ は R の左イデアルであり，$A_1, A_2, \cdots, A_n$ のすべてを含み，しかもそのような R の左イデアルの中で最も小さい．

特に，単項左イデアル $(a_1), (a_2), \cdots, (a_n)$ の和 $(a_1)+(a_2)+\cdots+(a_n)$ は

$$\{x_1a_1+x_2a_2+\cdots+x_na_n \mid x_1, x_2, \cdots, x_n\in R\}$$

であり，これはまた $a_1, a_2, \cdots, a_n$ を含む最小の R の左イデアルでもある．これを $a_1, a_2, \cdots, a_n$ から**生成**された R の左イデアルとよぶ．

同じように R の左イデアル $A_1, A_2, \cdots, A_n$ に対して，共通部分

$$A_1\cap A_2\cap\cdots\cap A_n$$

も R の左イデアルであり，$A_1, A_2, \cdots, A_n$ のいずれにも含まれる R の左イデアルの中で最も大きい．この例の詳しい証明は演習問題とする．

例 4　$a_1, a_2, \cdots, a_n$ を $\boldsymbol{Z}$ の元とする．この中に0でないものがあれば，$a_1, a_2, \cdots, a_n$ の最大公約数 d が存在して

$$(a_1)+(a_2)+\cdots+(a_n)=(d)$$

であることを1.5節でのべた．ここで加法群 $\boldsymbol{Z}$ の部分群は $\boldsymbol{Z}$ のイデアルと同

じ概念であったことに注意. (d) は，したがって，$(a_1), (a_2), \cdots, (a_n)$ のすべてを含む $\boldsymbol{Z}$ のイデアルの中で最も小さい.

同じようにして，$a_1, a_2, \cdots, a_n$ のすべてが 0 でないときは，$a_1, a_2, \cdots, a_n$ の最小公倍数 l が存在して

$$(a_1) \cap (a_2) \cap \cdots \cap (a_n) = (l)$$

が成り立つ. (l) は $(a_1), (a_2), \cdots, (a_n)$ のいずれにも含まれる $\boldsymbol{Z}$ のイデアルの中で最も大きい.

例 5 2.1 節例 3 の環 R において，$x \in X$ に対し

$$\{f \in R \mid f(x) = 0\}$$

は R のイデアルである.

2.1 節例 2 の環 R では

$$\left\{\begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} \middle| \, b, d \in R\right\}$$

は R の左イデアルであり，

$$\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| \, a, b \in R\right\}$$

は R の右イデアルである. これらの証明はいずれも演習問題とする.

定理 2.4 環 R に対して，次の条件は同値である.

(1) R は斜体である.

(2) R の左イデアルはすべて自明である.

(3) R の右イデアルはすべて自明である.

証明 (1) ⇒ (2): A を R の左イデアルで $\{0\}$ でないとする. A は 0 でない元 a を含み，したがって，$1 = a^{-1} \cdot a \in A$ で $A = R$ となる.

(2) ⇒ (1): $R \ni a \neq 0$ とすると，仮定から a から生成された R の左イデアル (a) は R に等しい. したがって，$ba = 1$ をみたす R の元 b が存在する. $b \neq 0$ から b から生成された R の左イデアル (b) も R と一致し，$cb = 1$ をみたす R の元 c がある. このとき，$a = cb \cdot a = c \cdot ba = c$ から $ab = ba = 1$ となり，a は単元である.

(1) と (3) の同値も同じように証明できる.

例 6 そのイデアルがすべて自明である環を**単純環**とよぶ. 定理 2.4 から

体は単純環である

ことが分かるが，R が可換環ならば

$$R \text{ が体} \iff R \text{ は単純環}$$

が成り立つ．この証明は演習問題とする．

2.1 節例 2 の環 $(\boldsymbol{R})_2$ について

$$(\boldsymbol{R})_2 \text{ は単純環ではあるが，斜体ではない}$$

ことを示す．斜体でないことは明らかで，単純環であることを示すために，$(\boldsymbol{R})_2$ の $\{0\}$ でないイデアルを A とし，$A \ni \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \neq 0$ とする．$a_{11} \neq 0$ のときは

$$A \ni \begin{pmatrix} \frac{1}{a_{11}} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

$$A \ni \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

であるから，$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in A$ となる．このことは $A = (\boldsymbol{R})_2$ を意味し，$(\boldsymbol{R})_2$ は自明なイデアルしかもたないことが分かる．

$a_{11}=0$ の場合の証明は演習問題とする．

$\boldsymbol{R}$ の上の $n \times n$ 行列全体のつくる環を $(\boldsymbol{R})_n$ とかけば，$(\boldsymbol{R})_n$ も同じように単純環ではあるが，斜体ではない．

A を環 R のイデアルとする．A は加法群 R の正規部分群であるから，剰余群 R/A がつくれる．この剰余群の演算は加法であって 2 つの元 $a+A, b+A$ の和は

$$(a+A)+(b+A)=(a+b)+A$$

で与えられていた．いま写像 φ を

$$\varphi\colon R/A \times R/A \to R/A, \quad (a+A, b+A) \to ab+A$$

ときめる．この φ が一意写像であることを示す．

$a, a', b, b' \in R$ に対して，$a+A=a'+A$，$b+A=b'+A$ ならば，$a-a' \in A$，$b-b' \in A$ であり，

$$ab-a'b'=a(b-b')+(a-a')b' \in A.$$

したがって，$ab+A=a'b'+A$ で φ は一意写像である．

この φ を用いて R/A の 2 元 $a+A, b+A$ の積を

$$(a+A)\cdot(b+A)=ab+A$$

ときめる．φ が一意写像であることは，この積が代表元 a, b のとり方に依存しないできまることを示している．

R/A は上の2つの演算に関して環をつくる．この環を R の A による**剰余環**とよぶ．R/A の元 $a+A$ を簡単に $\bar{a}$ とかくことがある．このとき，R/A の零元は $\bar{0}=0+A$ であり，単位元は $\bar{1}=1+A$ である．

自明なイデアルによる剰余環がどんな環であるかを調べておこう．$A=R$ のとき $1-0\in R=A$ であるから，$\bar{1}=\bar{0}$ となり剰余環 R/A は零環となる．このような環を考えないことはすでに約束した (2.1節参照)．

また，$A=\{0\}$ のときは，1.3節例8のように R の元 a と a の属する剰余類 $\bar{a}$ とを同一視して，R と R/A とは同じものと考える．

例 7　$\boldsymbol{Z}$ の $\{0\}$ でないイデアルはある自然数 m によって (m) とあらわされる．$\boldsymbol{Z}$ の (m) による剰余環 $\boldsymbol{Z}/(m)$ の加法は，加法群 $\boldsymbol{Z}$ の (m) による剰余群 $\boldsymbol{Z}/(m)$ の加法である．1.3節例7によれば，$\boldsymbol{Z}/(m)$ の2元 $\bar{i}, \bar{j}$ $(0\leqq i,j\leqq m-1)$ の和は

$$i+j=mq+r \qquad (0\leqq r<m)$$

とかいたとき

$$\bar{i}+\bar{j}=\bar{r}$$

ときめた．$\boldsymbol{Z}/(m)$ の乗法もまた同じで

$$i\cdot j=mq'+r' \qquad (0\leqq r'<m)$$

とかいたとき

$$\bar{i}\cdot\bar{j}=\bar{r}'$$

ときめればよい．例えば，$m=6$ のとき，剰余環 $\boldsymbol{Z}/(6)=\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ の乗法の乗積表は表2.1のようになる．

表 2.1

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

例 8　m を自然数として $\boldsymbol{Z}$ の (m) による剰余環 $\boldsymbol{Z}/(m)$ では，$\bar{a}\neq 0$ に対して

$$\bar{a}\text{ が }\boldsymbol{Z}/(m)\text{ の単元} \quad \Leftrightarrow \quad (a, m)=1,$$
$$\bar{a}\text{ が }\boldsymbol{Z}/(m)\text{ の零因子} \quad \Leftrightarrow \quad (a, m)\neq 1$$

が成り立つ．ここで (a, m) は a と m の最大公約数をあらわす．

実際，$(a, m)=1$ ならば，$ax+my=1$ をみたす $x, y\in \boldsymbol{Z}$ が存在する（1.5節参照）．このとき

$$\bar{a}\cdot\bar{x}=\bar{a}\bar{x}+\bar{m}\bar{y}=\bar{1}$$

であり，$\bar{a}$ は $\boldsymbol{Z}/(m)$ の単元である．

$(a, m)\neq 1$ のとき，$(a, m)=d$ とおき

$$a=da', \quad m=dm'$$

とかけば，

$$\bar{a}\cdot\bar{m}'=\overline{da'}\cdot\bar{m}'=\bar{m}\cdot\bar{a}'=\bar{0}.$$

$\bar{m}'\neq 0$ であるから，$\bar{a}$ は $\boldsymbol{Z}/(m)$ の零因子である．

逆に，$\bar{a}$ が単元ならば，$\bar{a}$ は零因子でありえず $(a, m)=1$ であり，$\bar{a}$ が零因子ならば，$\bar{a}$ は単元ではありえず $(a, m)\neq 1$ である．

m を法とする剰余類 $\bar{a}$ で $(a, m)=1$ であるものを m を法とする既約剰余類とよんだ（1.5節参照）．既約剰余類の全体が乗法に関して群をつくることも1.5節でのべたが，このことは上にのべたことから

環の単元の全体が乗法に関して群をつくる

という命題の特別な場合であるということもできる．この命題の証明は演習問題とする．

例 9　例8から

$$m\text{が素数} \iff \boldsymbol{Z}/(m)\text{は体},$$
$$m\text{が合成数} \iff \boldsymbol{Z}/(m)\text{は零因子をもつ}$$

が成り立つ．

実際，m が素数で，$\bar{0}\neq\bar{a}\in\boldsymbol{Z}/(m)$ とすると，$m\nmid a$ から $(a, m)=1$．したがって，$\bar{a}$ は $\boldsymbol{Z}/(m)$ の単元で，これは $\boldsymbol{Z}/(m)$ が体であることを示している．

m が合成数のときは，$1<m'<m$ なる約数 m' がある．$m=m'm''$ とかけば，$\boldsymbol{Z}/(m)$ で $\bar{m}'\neq\bar{0}, \bar{m}''\neq\bar{0}$，かつ $\bar{m}'\cdot\bar{m}''=\bar{m}=\bar{0}$ であるから $\bar{m}'$ は零因子である．

逆の証明は例8と同じようにしてできる．

2.3　環の準同型

環 R から環 R' への一意写像 $f\colon R\to R'$ が，R の任意の2元 a, b に対して

$$f(a+b)=f(a)+f(b),$$

$$f(ab)=f(a)f(b)$$

をみたし，その上，

$$f(1)=1'$$

であるとき，f を R から R' への**環準同型写像**または単に**環準同型**とよぶ．ここで $1, 1'$ はそれぞれ R, R' の単位元をあらわす．

準同型 f が，単射ならば f を**単射環準同型**，全射ならば**全射環準同型**とよぶ．特に，全単射環準同型 f を**環同型**とよぶ．R から R' への環同型 f が存在するとき，R と R' は環同型であるといい，$R \cong^f R'$ または単に $R \cong R'$ とかく．

環準同型 $f: R \to R'$ は加法群の準同型でもあるから，補題 1.15 を用いて，任意の $a, b \in R$ に対して $f(a+(-b))=f(a)+f(-b)=f(a)+(-f(b))$ であり，

$$f(a-b)=f(a)-f(b)$$

が成り立つ．

R, R' を環，$f: R \to R'$ を環準同型とする．f による R の像 $f(R)$ を単に f の**像**とよぶ．補題 2.2 から $f(R)$ は R' の部分環をつくることが分かる．R' の零元 $0'$ の f による原像

$$f^{-1}(0')=\{a \in R \mid f(a)=0'\}$$

を f の**核**とよび，$\mathrm{Ker}\, f$ であらわす．$\mathrm{Ker}\, f$ は R のイデアルをつくり，群のときと同じように

$$f \text{ が全射} \Leftrightarrow f \text{ の像} = R',$$
$$f \text{ が単射} \Leftrightarrow f \text{ の核} = \{0\}$$

が成り立つ．ここで 0 は R の零元をあらわす．

例 1　写像 f を

$$f: \boldsymbol{C} \to \boldsymbol{C}, \quad z=a+bi \to a-bi$$

ときめる．f は一意写像である．複素数 $z=a+bi$ に対し，$a-bi$ を $\bar{z}$ とかき，z の共役複素数とよぶ．2 つの複素数 z, z' に対して

$$\overline{z+z'}=\bar{z}+\bar{z}', \quad \overline{z \cdot z'}=\bar{z} \cdot \bar{z}'$$

が成り立つ．その上，実数 a を複素数とみたとき，a の共役複素数は a と一致する．このことは f が環準同型であることを示している．

一方，任意の複素数 z に対して

$$\bar{\bar{z}}=z$$

が成り立つから f は全射であり，また単射でもある．したがって，f は環同型である．

同じようなことはガウスの整数環 $\boldsymbol{Z}[i]$ でも成り立つ．

例 2　4元数環Rで

$$R' = \{aE+bJ \mid a, b \in \boldsymbol{R}\} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| \, a, b \in \boldsymbol{R} \right\}$$

がRの部分環をつくることは，補題2.2を用いて確かめられる．写像fを

$$f\colon R' \to \boldsymbol{C}, \quad \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \to a+bi$$

ときめれば，fは一意写像であり，環同型であることも容易に分かる．

例 3　環Rの元aに対して，写像a_Lを

$$a_L\colon R \to R, \quad x \to ax$$

ときめる．a_Lは一意写像であり，Rの任意の2元x, yに対して，分配法則

$$a\cdot(x+y) = ax+ay$$

はa_Lが加法群Rの自己準同型であることを示している．このとき，写像fを

$$f\colon R \to \mathrm{End}(R), \quad a \to a_L$$

ときめれば，fは一意写像であり，単射環準同型である．

実際，Rの2元a, bに対して，$a_L = b_L$ならば，Rの単位元1に施して$a = a_L(1) = b_L(1) = b$をうる．したがって，fは単射である．

一方，Rの元a, b, xに対して

$$(a+b)_L(x) = (a+b)x = ax+bx = a_L(x)+b_L(x) = (a_L+b_L)(x),$$
$$(ab)_L(x) = (ab)x = a(bx) = (a_L\cdot b_L)(x),$$
$$1_L(x) = 1\cdot x = x$$

が成り立つことは，fが環準同型であることを示している．

fが単射環準同型であることは，$R \cong^f f(R)$であり，$f(R)$は$\mathrm{End}(R)$の部分環であるから

任意の環Rは$\mathrm{End}(R)$の部分環と環同型である．

特に，$R = \boldsymbol{Z}$とし，加法群$\boldsymbol{Z}$の任意の自己準同型を$g\colon \boldsymbol{Z} \to \boldsymbol{Z}$とする．$g(1) = a$とおけば，$\boldsymbol{Z}$の任意の元$b$に対して

$$g(b) = b\cdot g(1) = ab$$

が成り立つから，$g = a_L$となる．したがって，$f\colon \boldsymbol{Z} \to \mathrm{End}(\boldsymbol{Z})$は全射環準同型で

$$\boldsymbol{Z} \cong^f \mathrm{End}(\boldsymbol{Z})$$

が成り立つ．

例 4　$f\colon R \to R'$が環Rから環R'への環準同型ならば，$\mathrm{Ker}\, f$はRのイデアルであった．逆に，

$$R\text{のイデアルはすべて適当な環準同型の核である}$$

ことを示す(1.4 節例 8 参照).

AをRのイデアルとし，剰余環 R/A をつくる．R/A は，もともとは加法群 Rの部分群Aによる剰余群であって，加法群Rから剰余群 R/A への標準的準同型 (1.4 節例 4)

$$\pi: R \to R/A, \quad a \to a+A$$

の核は

$$\mathrm{Ker}\,\pi = \{a \in R \mid a+A=0+A\} = A$$

であった (1.4 節例 8)．剰余環 R/A の乗法は，Rの元 a, b に対して $(a+A)\cdot(b+A)=ab+A$ ときめたが，このことは

$$\pi(a)\pi(b)=\pi(ab)$$

を意味し，しかも

$$\pi(1)=1+A$$

でもあるから，π は環Rから剰余環 R/A への環準同型で，イデアルAはこの π の核になっている．π をRから R/A への**標準的環準同型**または**自然な環準同型**という．

定理 2.5 (環の準同型定理) R, R' を環，$f: R \to R'$ を環準同型とする．f から誘導された写像

$$\bar{f}: R/\mathrm{Ker}\,f \to R', \quad \bar{a}=a+\mathrm{Ker}\,f \to f(a)$$

は単射環準同型で，したがって，

$$R/\mathrm{Ker}\,f \cong^{\bar{f}} f(R)$$

が成り立つ．

証明 R/A の 2 元 $\bar{a}, \bar{b}$ に対して，f が環準同型であることから

$$\bar{f}(\bar{a}+\bar{b})=\bar{f}(\overline{a+b})=f(a+b)=f(a)+f(b)=\bar{f}(\bar{a})+\bar{f}(\bar{b}),$$
$$\bar{f}(\bar{a}\cdot\bar{b})=\bar{f}(\overline{ab})=f(ab)=f(a)f(b)=\bar{f}(\bar{a})\bar{f}(\bar{b}),$$
$$\bar{f}(\bar{1})=f(1)=1'$$

が成り立ち，したがって，$\bar{f}$ は環準同型である．ここで $1'$ は R' の単位元をあらわす．明らかに，$\bar{f}$ は単射でもある．

例 5 $\boldsymbol{R}$ の上の三角行列環 (2.1 節例 11) と同じように，体Kの上の三角行列環Rを

$$R=\left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| \, a, b, c \in K\right\}$$

ときめ，簡単にこのRを$\begin{pmatrix} K & K \\ 0 & K \end{pmatrix}$であらわす．演習問題22から$R$の自明でないイデアルは

$$A_1=\begin{pmatrix} 0 & K \\ 0 & 0 \end{pmatrix},\quad A_2=\begin{pmatrix} 0 & K \\ 0 & K \end{pmatrix},\quad A_3=\begin{pmatrix} K & K \\ 0 & 0 \end{pmatrix}$$

でつくされる．ここで$\begin{pmatrix} 0 & K \\ 0 & 0 \end{pmatrix}=\left\{\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}\middle| b\in K\right\}$であり，他のものも同じように定義する．写像$f_2$を

$$f_2\colon R\to K,\quad \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\to a$$

ときめると，f_2は一意写像であり，全射環準同型でもあって

$$\mathrm{Ker}\, f_2=\left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\in R \;\middle|\; a=0\right\}=A_2.$$

したがって，定理2.5から

$$R/A_2 \cong^{\bar{f}_2} K.$$

同じようにして

$$R/A_3\cong K.$$

写像f_1を

$$f_1\colon R\to K\times K,\quad \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\to (a, c)$$

ときめる．ここで$K\times K$はKとKの直積（演習問題10）である．f_1は一意写像であり，また全射環準同型でもあって，その核は

$$\mathrm{Ker}\, f_1=\left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\in R \;\middle|\; a=c=0\right\}=A_1.$$

したがって，

$$R/A_1 \cong^{\bar{f}_1} K\times K.$$

例 6　m, nを互いに素な自然数とし，剰余環$\boldsymbol{Z}/(m)$と$\boldsymbol{Z}/(n)$との直積$\boldsymbol{Z}/(m)\times\boldsymbol{Z}/(n)$を考える．写像$f$を

$$f\colon \boldsymbol{Z}\to \boldsymbol{Z}/(m)\times\boldsymbol{Z}/(n),\quad a\to (a+(m), a+(n))$$

ときめれば，fは一意写像であり，また環準同型でもある．fの核は

$$\mathrm{Ker}\, f=\{a\in\boldsymbol{Z} \mid a\in(m)\cap(n)\}=(mn)$$

で与えられる．したがって，定理2.5から

$$\boldsymbol{Z}/(mn)\cong f(\boldsymbol{Z})$$

であるが,

$$|f(\boldsymbol{Z})|=|\boldsymbol{Z}/(mn)|=mn=|\boldsymbol{Z}/(m)|\cdot|\boldsymbol{Z}/(n)|=|\boldsymbol{Z}/(m)\times\boldsymbol{Z}/(n)|$$

であるから, f は全射で

$$\boldsymbol{Z}/(mn)\cong\boldsymbol{Z}/(m)\times\boldsymbol{Z}/(n)$$

が成り立つ.

例 7 Rを環, その単位元を (数の 1 と区別して) e とかく. 写像fを

$$f\colon \boldsymbol{Z}\to R, \quad n\to ne$$

ときめる. fは一意写像である. 整数 m, n に対して

$$(m+n)e=me+ne, \quad (mn)e=me\cdot ne, \quad 1e=e$$

であるから, fは環準同型である. 上の第 1 式は定理 1.4 の指数法則を加法群Rに適用してえられ, 第 2 の式は分配法則による.

その上, $\boldsymbol{Z}$からRへの任意の環準同型は 1 を e にうつし, $n=n\cdot 1$ を ne にうつすからfと一致する. したがって, $\boldsymbol{Z}$からRへの環準同型はfしかない.

fの像$f(\boldsymbol{Z})=\{ne \mid n\in\boldsymbol{Z}\}$ はRの部分環であり, Rの部分環はすべてeを含むから$f(\boldsymbol{Z})$を含み, したがって, $f(\boldsymbol{Z})$はRの最小の部分環である.

$\mathrm{Ker}\, f$は$\boldsymbol{Z}$のイデアルであるから, $\mathrm{Ker}\, f=(m)$ となるmがきまる. mは 0 または自然数で, このmをRの**標数**とよぶ. $\mathrm{Ker}\, f=\{n\in\boldsymbol{Z} \mid ne=0\}$ であるから, Rの標数とは, 0 でない場合は, Rを加法群とみたときの e の位数にほかならない (1.4 節例 7).

Rの標数が 0 ならば, $f(\boldsymbol{Z})$は$\boldsymbol{Z}$と環同型であり, Rの標数がmならば, $f(\boldsymbol{Z})$は$\boldsymbol{Z}/(m)$と環同型である. このとき, mは 1 ではない. 実際, $m=1$ ならば, $e=1\cdot e=0$ でRは零環となる (2.1 節参照).

例 8 $\boldsymbol{Z}$では, 例 7 の環準同型$f\colon \boldsymbol{Z}\to\boldsymbol{Z}$は$\boldsymbol{Z}$の恒等写像にほかならない. したがって, $\mathrm{Ker}\, f=(0)$ で, $\boldsymbol{Z}$の標数は 0 である.

同じようにして, $\boldsymbol{Q}, \boldsymbol{R}, \boldsymbol{C}$の標数もすべて 0 である.

例 9 自然数mに対して, 剰余環 $\boldsymbol{Z}/(m)$ では例 7 の環準同型$f\colon \boldsymbol{Z}\to\boldsymbol{Z}/(m)$は

$$f(n)=n\cdot 1+(m)=n+(m)$$

で標準的な環準同型πに一致する. したがって, $\mathrm{Ker}\, f=(m)$ で$\boldsymbol{Z}/(m)$の標数はmである.

例 10 整域Rの標数mは 0 かまたは素数である.

実際, $m\neq 0$ のとき, 例 7 の環準同型 $f\colon \boldsymbol{Z}\to R$ の像$f(\boldsymbol{Z})$はRの部分環として整域であり, $\mathrm{Ker}\, f=(m)$, $\boldsymbol{Z}/(m)\cong f(\boldsymbol{Z})$ であるから$\boldsymbol{Z}/(m)$も零因子を

もちえない．mは素数である (2.2 節例 9)．

Rを環，AをRのイデアルとし，剰余環R/Aの左イデアルがどんなものであるかを，定理 1.20 を用いて調べてみよう．

$\pi: R \to R/A$ を標準的な環準同型とし，A' を R/A の左イデアルとする．A' は加法群Rの部分群Aによる剰余群 R/A の部分群である (2.2 節参照)．π は標準的な (加法群としての) 準同型でもあるから，定理 1.20 から $\pi^{-1}(A')$ はAを含むRの部分群で

$$A' = \pi^{-1}(A')/A = \{a+A \in R/A \mid a \in \pi^{-1}(A')\}$$

が成り立つ．ここで $\pi^{-1}(A')$ は環Rの左イデアルでもある．

逆に，Aを含むRの左イデアルBに対して

$$B/A = \{b+A \in R/A \mid b \in B\}$$

は定理 1.20 から R/A の部分群ではあるが，R/A の左イデアルにもなっている．したがって，次の定理が成り立つ．

定理 2.6　Rを環，AをRのイデアル，$\pi: R \to R/A$ を標準的な環準同型とする．このとき，

(1)　R/A の任意の左イデアル A' に対して，π による A' の原像 $\pi^{-1}(A')$ はAを含むRの左イデアルで，

$$A' = \pi^{-1}(A')/A.$$

(2)　Aを含むRの任意の左イデアルBに対して

$$B/A = \{b+A \in R/A \mid b \in B\}$$

は R/A の左イデアルである．

(3)　R/A の左イデアル A' とAを含むRの左イデアルBとに対して

$$A' \to \pi^{-1}(A')$$
$$B/A \leftarrow B$$

は，R/A の左イデアルの全体とAを含むRの左イデアルの全体との間の全単射を与える．

(4)　(3) の対応で

$$B/A \text{ が } R/A \text{ のイデアル} \Leftrightarrow B \text{ が } R \text{ のイデアル}$$

であり，このとき

$$(R/A)/(B/A) \cong R/B$$

が成り立つ．

証明　定理 1.20 から (4) のみ示せばよい，前半は B/A が R/A のイデアル

$\Leftrightarrow$ 任意の $b\in B, a\in R$ に対して $(b+A)\cdot(a+A)\in B/A \Leftrightarrow$ 任意の $b\in B, a\in R$ に対して $ba\in B \Leftrightarrow B$ が R のイデアルであり，後半は定理 1.20 の写像

$$f: R/A \to R/B, \quad a+A \to a+B$$

が乗法も保存し，したがって，環準同型であることに注意したらよい．

例 11 m を自然数 (>1) とする．(m) を含む $\boldsymbol{Z}$ のイデアルは (n) (n は m の正の約数) でつくされるから，$\boldsymbol{Z}/(m)$ のイデアルは m の正の約数の個数だけ存在する．

例えば，$\boldsymbol{Z}/(12)$ では，12の正の約数は

$$1, 2, 3, 4, 6, 12$$

で，$\boldsymbol{Z}/(12)$ のイデアルは

$$\boldsymbol{Z}/(12), (2)/(12), (3)/(12), (4)/(12), (6)/(12), (12)/(12)$$

の 6 個ある．ここで

$$(2)/(12)=\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}\},$$
$$(4)/(12)=\{\bar{0}, \bar{4}, \bar{8}\}$$

であるから，$(2)/(12)\supseteqq(4)/(12)$ が成り立つ．この意味の大小関係を図であらわすと図 2.1 のようになる．

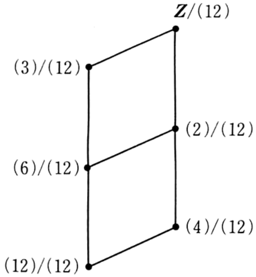


図 2.1

また，p を素数とするとき，剰余環 $\boldsymbol{Z}/(p)$ のイデアルは，上と同じ理由で

$$\boldsymbol{Z}/(p), \quad (p)/(p)$$

の自明なものしかない．$\boldsymbol{Z}/(p)$ は，したがって，可換な単純環で体をつくる (2.2 節例 6)．

$n\geqq 1$ に対して，剰余環 $\boldsymbol{Z}/(p^n)$ のイデアルは上と同じ理由で $\boldsymbol{Z}/(p^n)$, $(p)/(p^n), \cdots, (p^n)/(p^n)$ の $(n+1)$ 個でつくされ，

$$\boldsymbol{Z}/(p^n)\supseteqq(p)/(p^n)\supseteqq(p^2)/(p^n)\supseteqq\cdots\supseteqq(p^{n-1})/(p^n)\supseteqq(p^n)/(p^n)$$

のような大小関係がある．

例 12　Rは環，Aはそのイデアルで$A \neq R$とする．Aを含むイデアルがAとRしかないとき，AをRの**極大イデアル**とよぶ．Rが可換環ならば，2.2節例6から

$$A\text{が}R\text{の極大イデアル} \Leftrightarrow R/A\text{が体}$$

を意味する．例11の(p)は$\boldsymbol{Z}$の極大イデアルである．このほか，2.2節例5のイデアル$\{f \in R \mid f(x)=0\}$，この節の例5のイデアルA_2, A_3も極大イデアルである．これらの極大性の証明は演習問題とする．

2.4 商　　体

Kを体，RをKの部分環とする．Kは乗法に関して可換であるからRもそうであり，Kは零因子をもたないからRももたない．したがって，Rは整域である．

$a, b \in R$で$b \neq 0$とする．aと，bのKにおける逆元b^{-1}とのKにおける積ab^{-1}の全体

$$L=\{ab^{-1} \in K \mid a, b \in R, b \neq 0\}$$

はRを含むKの部分体をつくる．

LがRを含むことは$b=1$をとってみれば分かる．Lが部分体をつくることは，Lの2元$ab^{-1}, a'(b')^{-1}$に対して

$$ab^{-1}-a'(b')^{-1}=(ab'-a'b)\cdot(bb')^{-1}$$

であり，$a'(b')^{-1} \neq 0$のときは$a' \neq 0$であって

$$ab^{-1}\cdot(a'(b')^{-1})^{-1}=ab'\cdot(a'b)^{-1}$$

であることから分かる (補題2.3)．

定理 2.7　Kが体，RがKの部分環ならば，Rは整域で

$$L=\{ab^{-1} \in K \mid a, b \in R, b \neq 0\}$$

はRを含むKの最小の部分体である．

証明　最小性を示せばよい．K'をRを含むKの任意の部分体とする．Lの元ab^{-1}を任意にとる．$a, b \in K', b \neq 0$とみれば$ab^{-1} \in K'$ (補題2.3)．したがって，$L \subseteqq K'$である．

例 1　$\boldsymbol{Q}$は体，$\boldsymbol{Z}$は$\boldsymbol{Q}$の部分環である．$\boldsymbol{Z}$を含む$\boldsymbol{Q}$の最小の部分体Lは

$$\left\{\frac{a}{b} \in \boldsymbol{Q} \mid a, b \in \boldsymbol{Z}, b \neq 0\right\}$$

で $\boldsymbol{Q}$ に等しい．このことは $\boldsymbol{Z}$ と $\boldsymbol{Q}$ の間には $\boldsymbol{Q}$ 以外に体が存在しないことを示している．

例 2　体Kのすべての部分体の共通部分 k はまたKの部分体であり，Kの最小の部分体である．この意味で k はKによって一意的にきまる．この k をKの**素体**とよぶ．

Kの単位元を e とかき，2.3 節例 7 の環準同型

$$f\colon \boldsymbol{Z} \to K, \quad n \to ne$$

を考える．f の像 $f(\boldsymbol{Z})$ はKの最小の部分環であったから $f(\boldsymbol{Z}) \subseteqq k$ である．$f(\boldsymbol{Z})$ を含むKの最小の部分体Lは

$$\{ne\cdot(me)^{-1} \in K \mid n, m \in \boldsymbol{Z}, me \neq 0\}$$

で，$L \subseteqq k$ であるが，k の最小性から $L=k$ が成り立つ．すなわち，

体Kの素体 k は $f(\boldsymbol{Z})$ を含むKの最小の部分体Lに等しい．

例 3　体Kが $\boldsymbol{Q}$ のときは, 例 2 の環準同型 $f\colon \boldsymbol{Z} \to \boldsymbol{Q}$ は包含写像となるから, $\boldsymbol{Q}$ の素体 k は $\boldsymbol{Z}$ を含む $\boldsymbol{Q}$ の最小の部分体 $\boldsymbol{Q}$ 自身に等しい. 同じようにして $\boldsymbol{R}$, $\boldsymbol{C}$ の素体も $\boldsymbol{Q}$ に等しい.

定理 2.8　体Kの素体 k は

Kの標数が 0 ならば，$\boldsymbol{Q}$ と環同型，

Kの標数が p ならば，$\boldsymbol{Z}/(p)$ と環同型

である．

証明　Kの標数が 0 のとき，例 2 の環準同型 $f\colon \boldsymbol{Z} \to K$ は単射 (2.3 節例 7) であり，これを拡張して，写像

$$g\colon \boldsymbol{Q} \to K, \quad \frac{n}{m} \to f(n)f(m)^{-1} = ne(me)^{-1}$$

を考える．$\boldsymbol{Q}$ の 2 元 $\dfrac{n}{m}, \dfrac{n'}{m'}$ に対して

$$\begin{aligned}\frac{n}{m} = \frac{n'}{m'} &\Leftrightarrow nm' = n'm \\ &\Leftrightarrow f(n)f(m') = f(n')f(m) \\ &\Leftrightarrow f(n)f(m)^{-1} = f(n')f(m')^{-1}\end{aligned}$$

となって，g は一意写像であり，かつ単射でもある．g が環準同型であることの証明は演習問題とする．g の像はLに等しい(例 2)から

$$\boldsymbol{Q} \cong^{g} L = k.$$

Kの標数が p のときは，$f(\boldsymbol{Z})$ は $\boldsymbol{Z}/(p)$ と環同型であり (2.3 節例 7),

$\boldsymbol{Z}/(p)$ が体をつくるから $f(\boldsymbol{Z})$ も体で，$f(\boldsymbol{Z})=L=k$, $\boldsymbol{Z}/(p)\cong k$ である．

体の部分環は整域であったが，次の定理はどんな整域もある体の部分環とみられることを示している．

定理 2.9　R が整域ならば，体 M と単射環準同型 α: $R\to M$ とがあって

$$M=\{\alpha(a)\alpha(b)^{-1}\mid a, b\in R, b\neq 0\}$$

とあらわされる．

証明　$R^*=R-\{0\}$ とおき，R と R^* の直積集合 $R\times R^*$ の上の関係 $\sim$ を

$$(a, b)\sim(a', b') \Leftrightarrow ab'=a'b$$

によってきめる．

この関係が反射律 $(a, b)\sim(a, b)$，対称律 $(a, b)\sim(a', b') \Rightarrow (a', b')\sim(a, b)$ をみたすことは明らか．推移律をみたすことを確かめる．

$(a, b)\sim(a', b')$, $(a', b')\sim(a'', b'')$ とする．$ab'=a'b$, $a'b''=a''b'$ が成り立つ．このとき

$$ab'b''=(a'b)b''=(a''b')b,\quad (ab''-a''b)b'=0$$

であるが，$b'\neq 0$, R は整域であるから $ab''-a''b=0$, $ab''=a''b$ で $(a, b)\sim(a'', b'')$ をうる．

したがって，$\sim$ は $R\times R^*$ の上の同値関係で，$R\times R^*$ をこの同値関係によって類別した同値類の全体を M とかく．(a, b) の属する同値類を $[a, b]$ とかき，M の演算 φ_1 を

$$\varphi_1\colon M\times M\to M,\quad ([a, b], [a', b'])\to[ab'+a'b, bb']$$

ときめる．φ_1 が一意写像であることを示す．

$([a, b], [a', b'])=([c, d], [c', d'])$ を仮定する．$(a, b)\sim(c, d)$，$(a', b')\sim(c', d')$ であるから $ad=cb$，$a'd'=c'b'$．したがって，

$$(ab'+a'b)\cdot dd'=cb\cdot b'd'+c'b'\cdot bd=(cd'+c'd)\cdot bb'.$$

このことは $(ab'+a'b, bb')\sim(cd'+c'd, dd')$，$[ab'+a'b, bb']=[cd'+c'd, dd']$ であることを示している．

M のもう 1 つの演算 φ_2 を

$$\varphi_2\colon M\times M\to M,\quad ([a, b], [a', b'])\to[aa', bb']$$

ときめる．上と同じようにして φ_2 も一意写像であることが分かる．

$M\times M$ の元 $([a, b], [a', b'])$ の φ_1, φ_2 による像を

$$\varphi_1([a, b], [a', b'])=[a, b]+[a', b'],$$
$$\varphi_2([a, b], [a', b'])=[a, b]\cdot[a', b']$$

とかいて，すなわち，

$$[a, b]+[a', b']=[ab'+a'b, bb'],$$
$$[a, b]\cdot[a', b']=[aa', bb']$$

によってMの加法，乗法を定義する．このとき，Mは体をつくる．

Rの0でない元$b, b', b'', \cdots$に対して

$$[0, b]=[0, b']=[0, b'']=\cdots$$

が成り立ち，この元がMの零元となり，また

$$[b, b]=[b', b']=[b'', b'']=\cdots$$

が成り立ち，この元がMの単位元となる．

Mの元$[a, b]$の加法に関する逆元は$[-a, b]$であり，乗法に関する逆元は($[a, b]$が零元でないならば$a\neq 0$であるから) $[b, a]$である．Mが体をつくることの詳しい証明は演習問題とする．

写像αを

$$\alpha: R\to M, \quad a\to [a, 1]$$

ときめると，αは一意写像であり，単射環準同型でもある．

Mの任意の元$[a, b]$は

$$[a, b]=[a, 1]\cdot[1, b]=\alpha(a)\cdot\alpha(b)^{-1}$$

とあらわされるから，定理の後半が証明された．

定理 2.10　R, R'を整域，$g: R\to R'$を単射環準同型とする．R, R'に対して定理2.9の意味の体M, M'，単射環準同型$\alpha: R\to M, \alpha': R'\to M'$がきまる．このとき，単射環準同型

$$h: M\to M'$$

が存在して，$\alpha' g=h\alpha$が成り立つ．

gが全射ならば，hもまた全射である(図2.2参照)．

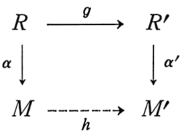


図 2.2

証明　写像hを

$$h\colon M\to M',\quad \alpha(a)\alpha(b)^{-1}\to\alpha'(g(a))\alpha'(g(b))^{-1}$$

ときめたらよい．ここで g が単射であるから $g(b)$ は 0 ではない．

定理 2.10 から整域 R に対して，定理 2.9 の体 M は同型を除いて一意的にきまる．この M を R の**商体**とよぶ．

この節のはじめにもどって，K を体，R を K の部分環とする．この R に対して，R を含む K の最小の部分体

$$L=\{ab^{-1}\in K\mid a,b\in R,\ b\neq 0\}$$

があり，また，R は整域であるから R の商体 M と単射環準同型 $\alpha\colon R\to M$ が存在する．このとき写像 α^* を

$$\alpha^*\colon L\to M,\quad ab^{-1}\to\alpha(a)\alpha(b)^{-1}$$

ときめると，α^* は一意写像で全単射であり，M の演算の定義から環同型にもなっている．詳しい証明は演習問題とする．

また，この α^* を R に制限すると α に一致している(図 2.3 参照)．

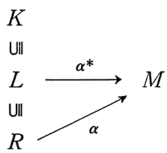


図 2.3

以後，簡単のために，R の元 a に対して a と $\alpha(a)$ を同一視する．このとき R の演算は M の演算と一致して R は M の部分環，M は R を含む体となり，L の元 ab^{-1} に対して

$$\alpha^*(ab^{-1})=\alpha(a)\alpha(b)^{-1}=ab^{-1}$$

が成り立つ．ここで最初の ab^{-1} は K における積，第 2 の ab^{-1} は M における積をあらわす．形は同じでも同じものかは分からない．

例 4　K を体，その素体を k とする．例 2 に上の同一視を適用すると

$$L=k\cong M.$$

特に，$K=\boldsymbol{Q}$ のときは，例 3 から

$$\boldsymbol{Q}=k\cong M$$

で，$\boldsymbol{Z}$ の商体は $\boldsymbol{Q}$ と同型である(図 2.4 参照)．

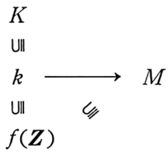


図 2.4

2.5 多項式環

実数を係数とする多項式の全体が環をなすことには2.1節例2で触れたが，この節ではもっと一般に，可換環Rの元を係数とする多項式を考える．

Rを可換環とし，Rの元の無限列

$$(a_0, a_1, a_2, \cdots)$$

で，ある番号nがあってnから先の元が

$$a_{n+1}=a_{n+2}=\cdots=0 \qquad (R\text{ の零元})$$

であるものを

$$f=(a_0, a_1, \cdots, a_n, 0, 0, \cdots)$$

とかいて，Rの元を係数とする**多項式**，またはRの上の多項式とよぶ．

Rの上の多項式の全体を簡単に$\bar{R}$とかこう．$\bar{R}$の2元

$$f=(a_0, a_1, \cdots, a_n, 0, 0, \cdots), \quad g=(b_0, b_1, \cdots, b_m, 0, 0, \cdots)$$

に対して，

$$f=g \Leftrightarrow \text{すべての } i \text{ に対して } a_i=b_i,$$

$$f+g=(a_0+b_0, a_1+b_1, a_2+b_2, \cdots),$$

$$f\cdot g=(a_0b_0, a_0b_1+a_1b_0, a_0b_2+a_1b_1+a_2b_0, \cdots)$$

ときめる．積$f\cdot g$を

$$f\cdot g=(c_0, c_1, c_2, \cdots)$$

とかけば，一般に，c_iは

$$c_i=\sum_{j=0}^{i} a_jb_{i-j}=\sum_{j+k=i} a_jb_k$$

とあらわされる．

fでは$a_{n+1}=a_{n+2}=\cdots=0$，gでは$b_{m+1}=b_{m+2}=\cdots=0$であるから，$l=\max\{n, m\}$とおけば，

$$a_{l+1}=a_{l+2}=\cdots=0, \quad b_{l+1}=b_{l+2}=\cdots=0$$

で，したがって，$f+g$では

$$a_{l+1}+b_{l+1}=a_{l+2}+b_{l+2}=\cdots=0$$

であって，$f+g$ も R の上の多項式である．

$f\cdot g$ では，$c_i=\sum_{j+k=i} a_jb_k$ において

$$i>n+m \Leftrightarrow j>n \text{ または } k>m \Leftrightarrow a_j=0 \text{ または } b_k=0$$

で，いずれにしても $i>n+m$ のときは

$$c_i=\sum_{j+k=i} a_jb_k=0$$

となるから，$f\cdot g$ もまた R の上の多項式である．

この加法，乗法に関して $\bar{R}$ は可換環をつくる．$\bar{R}$ の零元は

$$(0, 0, 0, \cdots)$$

であり，$\bar{R}$ の単位元は

$$(1, 0, 0, \cdots)$$

である．

例えば，$\bar{R}$ が乗法に関して結合法則をみたすことを確かめてみよう．$\bar{R}$ の元

$$f=(a_0, a_1, \cdots),\quad g=(b_0, b_1, \cdots),\quad h=(c_0, c_1, \cdots)$$

に対して，積 $(f\cdot g)\cdot h$ の第 n 成分は

$$\sum_{i+j=n}\left(\sum_{k+l=i} a_kb_l\right)\cdot c_j=\sum_{k+l+j=n}(a_kb_l)\cdot c_j$$

とあらわされる．この変形には R における右分配法則を用いている．同じように積 $f\cdot(g\cdot h)$ の第 n 成分は，R における左分配法則で

$$\sum_{k+i=n} a_k\cdot\left(\sum_{l+j=i} b_lc_j\right)=\sum_{k+l+j=n} a_k\cdot(b_lc_j)$$

とあらわされるから，R における結合法則を用いて

$$(f\cdot g)\cdot h=f\cdot(g\cdot h)$$

が成り立つ．$\bar{R}$ が可換環をつくることの証明は演習問題とする．

R から $\bar{R}$ への写像 θ を

$$\theta\colon R\to\bar{R},\quad a\to(a, 0, 0, \cdots)$$

ときめれば，θ は単射環準同型である．したがって，$(a, 0, 0, \cdots)$ を a と同一視して，R を $\bar{R}$ の部分環とみることができる．このとき

$$x=(0, 1, 0, 0, \cdots)$$

とおけば，

$$ax=(a, 0, 0, \cdots)\cdot(0, 1, 0, 0, \cdots)=(0, a, 0, 0, \cdots),$$
$$ax^2=(0, a, 0, 0, \cdots)\cdot(0, 1, 0, 0, \cdots)=(0, 0, a, 0, \cdots),$$
$$ax^3=(0, 0, a, 0, \cdots)\cdot(0, 1, 0, 0, \cdots)=(0, 0, 0, a, 0, \cdots)$$
$$\cdots$$

で，一般には，

$$ax^i=(0, 0, \cdots, 0, \overset{i+1}{\overset{\smile}{a}}, 0, 0, \cdots)$$

が成り立つ．したがって，$\bar{R}$ の任意の元

$$f=(a_0, a_1, \cdots, a_n, 0, 0, \cdots)$$

を

$$\begin{aligned}f&=(a_0, 0, 0, \cdots)+(0, a_1, 0, 0, \cdots)+\cdots+(0, \cdots, 0, a_n, 0, 0, \cdots)\\&=a_0+a_1x+\cdots+a_nx^n\end{aligned}$$

といわゆる多項式の形にかきなおせる．この意味で $\bar{R}$ の元 f は R の元を係数とする x の多項式であり，普通は $f(x)$ であらわす．

$\bar{R}$ を R の上の**多項式環**とよび，これからは $R[x]$ であらわす．R を $R[x]$ の**係数環**，x を**不定元**とよんでいる．

$R[x]$ の零元を**零多項式**とよぶ．これはすべての係数が R の零元である多項式

$$f(x)=0+0\cdot x+0\cdot x^2+\cdots$$

で，簡単に $f(x)=0$ であらわす．0 でない $R[x]$ の元には，ある n があって

$$f(x)=a_0+a_1x+\cdots+a_nx^n \qquad (a_n\neq 0)$$

とあらわされる．この n を $f(x)$ の**次数**とよび，$\deg f(x)$ であらわす．a_n を $f(x)$ の**最高次係数**とよび，特に，これが R の単位元 1 に等しいとき，$f(x)$ を**モニック**とよぶ．

次数が 0 の多項式は，いわゆる定数項のみの

$$f(x)=a_0 \qquad (a_0\neq 0)$$

の形をしている．これを**定数多項式**とよぶ．

零多項式も定数多項式 $f(x)=0$（0 は R の零元）とみることができるが，その次数は考えない．

上にのべた写像 θ: $R\to R[x]$ は R の元 a を定数多項式 $f(x)=a$（零多項式もこめて）にうつすものであり，a と $f(x)=a$ とを同一視して R を $R[x]$ の部分環とみている．

補題 2.11　$f(x), g(x)$ が共に 0 でない $R[x]$ の元ならば，

(1)　$f(x)+g(x)$ は 0 か，そうでなければ

$$\deg(f(x)+g(x))\leqq\max\{\deg f(x), \deg g(x)\}$$

が成り立つ．

(2) $f(x)\cdot g(x)$ は 0 か，そうでなければ

$$\deg(f(x)\cdot g(x)) \leqq \deg f(x) + \deg g(x)$$

が成り立つ．このとき，R が整域ならば，等号が成り立ち，したがって，

$$R \text{ が整域 } \Rightarrow R[x] \text{ も整域.}$$

証明

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \qquad (a_n \neq 0),$$
$$g(x) = b_0 + b_1 x + \cdots + b_m x^m \qquad (b_m \neq 0)$$

とおく．このとき，$\deg f(x) = n$，$\deg g(x) = m$ である．

(1) $f(x)+g(x)$ が 0 でないとする．$n=m$ のときは

$$f(x)+g(x) = (a_0+b_0) + (a_1+b_1)x + \cdots + (a_n+b_n)x^n$$

で，$a_n+b_n=0$ ならば，$\deg(f(x)+g(x)) < n$ であり，$a_n+b_n \neq 0$ ならば，$\deg(f(x)+g(x)) = n$ である．

$n>m$ のときは

$$f(x)+g(x) = (a_0+b_0) + (a_1+b_1)x + \cdots + (a_m+b_m)x^m + a_{m+1}x^{m+1} + \cdots + a_n x^n$$

で，$a_n \neq 0$ であるから，$\deg(f(x)+g(x)) = n$ である．

(2) $f(x)\cdot g(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \cdots + a_n b_m x^{n+m}$ が 0 でなければ，係数 $a_0 b_0, a_0 b_1 + a_1 b_0, \cdots, a_n b_m$ の中に 0 でないものがある．$a_n \neq 0$ であり，$b_m \neq 0$ であるが，$a_n b_m = 0$ のときは

$$\deg(f(x)\cdot g(x)) < n+m$$

である．R が零因子をもたないときは，$a_n b_m \neq 0$ で，したがって，

$$\deg(f(x)\cdot g(x)) = n+m.$$

このことは，$f(x), g(x)$ が 0 でないならば $f(x)\cdot g(x)$ も 0 でなく，R が整域ならば $R[x]$ も整域であることを示している．

例 1　$\boldsymbol{Z}$ の上の多項式

$$f(x) = 1+2x+3x^2, \quad g(x) = 2+x-3x^2$$

では $f(x)+g(x) = 3+3x$ で

$$\deg(f(x)+g(x)) < \max\{\deg f(x), \deg g(x)\}.$$

$\boldsymbol{Z}/(6)$ の上の多項式

$$f(x) = \bar{1}+\bar{2}x, \quad g(x) = \bar{3}+x+\bar{3}x^2$$

では，$f(x)\cdot g(x) = \bar{3}+x+\bar{5}x^2$ で

$$\deg(f(x)\cdot g(x)) < \deg f(x) + \deg g(x).$$

例 2　R を整域とし，多項式環 $R[x]$ の単元を求めてみよう．

明らかにRの単元は$R[x]$の単元である．逆に，$f(x)\in R[x]$が$R[x]$の単元ならば，$f(x)\cdot g(x)=1$をみたす$R[x]$の元$g(x)$が存在する．

$$0=\deg(f(x)\cdot g(x))=\deg f(x)+\deg g(x)$$

から，$f(x)$の次数は0でなければならない．このとき，$g(x)$の次数も0で，したがって，$R[x]$の単元はRの単元である．

Sを可換環，RをSの部分環とし，$R[x]$の元

$$f(x)=a_0+a_1x+\cdots+a_nx^n$$

とSの元cとに対して

$$f(c)=a_0+a_1c+\cdots+a_nc^n$$

ときめる．このSの元$f(c)$を$f(x)$のxにcを**代入**した元とよぶ．

次の補題の証明は演習問題とする．

補題 2.12 Sを可換環，RをSの部分環とし，$c\in S$とする．このとき，

(1) $R[x]$からSへの写像

$$h\colon R[x]\to S,\qquad f(x)\to f(c)$$

は環準同型である．

(2) $\mathrm{Ker}\,h=\{f(x)\in R[x]\mid f(c)=0\}$.

(3) hの像$h(R[x])=\{f(c)\mid f(x)\in R[x]\}$は$R$と$c$を含む$S$の最小の部分環である．

環準同型hは$R[x]$の定数多項式をそれ自身にうつすから，$\mathrm{Ker}\,h\neq R[x]$である．また，hの像$h(R[x])$をRの元を係数とするcの多項式の全体とみて，これを$R[c]$であらわす．

$f(c)=0$をみたすSの元cを多項式$f(x)$の**根**とよぶ．Rの上の多項式がRの中に根をもつとはかぎらない．Rが体のときは，Rを部分体として含むある体の中に$f(x)$は根をもつ(定理4.4参照)．

体Kの上の多項式環$K[x]$は整域であるから，定理2.9により，$K[x]$の商体が存在する．これを$K(x)$であらわす．2.4節で注意したように，$K[x]$を$K(x)$の部分環とみれば，

$$K(x)=\{f(x)\cdot g(x)^{-1}\mid f(x),g(x)\in K[x],g(x)\neq 0\}$$

とあらわされる．$K(x)$をKの上のxの**有理関数体**とよぶ．

定理 2.13 Kが体，$f(x),g(x)\in K[x]$で$\deg g(x)\geqq 1$とする．このとき

$$f(x)=g(x)\cdot q(x)+r(x),$$
$$r(x)=0 \text{ または } \deg r(x)<\deg g(x)$$

をみたす $q(x), r(x)\in K[x]$ がただ1組存在する.

証明　$f(x)=0$ または $f(x)\neq 0$ で $\deg f(x)<\deg g(x)$ のときは $q(x)=0$, $r(x)=f(x)$ とおけばよい. そこで

$$f(x)=a_0+a_1x+\cdots+a_nx^n \qquad (a_n\neq 0),$$
$$g(x)=b_0+b_1x+\cdots+b_mx^m \qquad (b_m\neq 0)$$

とおき, $n\geqq m$ とする. n に関する帰納法で $q(x), r(x)$ の存在を示す.

$n=1$ のときは $m=1$ で,

$$f(x)=(a_1b_1^{-1})\cdot g(x)+(a_0-a_1b_1^{-1}b_0)$$

から $q(x)=a_1b_1^{-1}$, $r(x)=a_0-a_1b_1^{-1}b_0$ とおけばよい.

n より小さな次数の多項式に対しては, $q(x), r(x)$ の存在を仮定して,

$$f_1(x)=f(x)-a_nb_m^{-1}x^{n-m}\cdot g(x)$$

をつくれば, x の n 乗の項が消えて $\deg f_1(x)<n$ となるから帰納法の仮定で

$$f_1(x)=g(x)\cdot q_1(x)+r_1(x)$$

をみたす $q_1(x), r_1(x)$ が $K[x]$ に存在する. ここで $r_1(x)=0$ かまたは $\deg r_1(x)<m$ である. このとき

$$g(x)\cdot(q_1(x)+a_nb_m^{-1}x^{n-m})+r_1(x)=f_1(x)+(f(x)-f_1(x))=f(x)$$

であるから, $q(x)=q_1(x)+a_nb_m^{-1}x^{n-m}$, $r(x)=r_1(x)$ ときめればよい.

次に, $q(x), r(x)$ の一意性を示す. $q(x), r(x)$ のほかに条件をみたす $q_2(x)$, $r_2(x)$ があったとする.

$$f(x)=g(x)\cdot q(x)+r(x)=g(x)\cdot q_2(x)+r_2(x)$$

であるから, $g(x)\cdot(q(x)-q_2(x))=r_2(x)-r(x)$ となる. もし $q(x)-q_2(x)\neq 0$ ならば, 左辺の次数 $\geqq m$, 右辺は0ではなくその次数 $<m$ となって矛盾する. したがって, $q(x)-q_2(x)=0$ であり, それから $r_2(x)-r(x)=0$ をうる. 条件をみたす $q(x), r(x)$ はただ1組しか存在しない.

$q(x), r(x)$ を, それぞれ, $f(x)$ を $g(x)$ で割ったときの**商**, **剰余**とよぶ.

定理2.13は多項式環における**除法の定理**とよばれている. $\boldsymbol{Z}$ においても同じような除法の定理が成り立ち(1.2節参照), したがって, $\boldsymbol{Z}$ が単項イデアル整域であることを証明した. 定理2.13を用いて体 K 上の多項式環 $K[x]$ が単項イデアル整域であることを証明できるが, もっと一般に,

整域 R の0でない各元 a に整数 $d(a)\geqq 0$ が対応していて

任意の0でないRの元a, bに対して

$$a=bq+r,\quad r=0 \text{ または } d(r)<d(b)$$

をみたすRの元q, rが存在するとき，Rを**ユークリッド整域**とよび，ユークリッド整域が単項イデアル整域であることを1.2節例10のようにして示すことができる．これは演習問題とする．

例 3 $\boldsymbol{Z}$や$K[x]$以外に$\boldsymbol{Z}[i]$，$\{a+b\sqrt{2}\mid a, b\in\boldsymbol{Z}\}$もユークリッド整域である．それをみるために，複素数$\alpha=a+bi$に対して，αの**ノルム**$N(\alpha)$を

$$N(\alpha)=a^2+b^2$$

ときめる．明らかに$N(\alpha)=0 \Leftrightarrow \alpha=0$であり，また$N(\alpha\beta)=N(\alpha)N(\beta)$が成り立つ．$0\neq\alpha\in\boldsymbol{Z}[i]$ならば$N(\alpha)$は自然数である．このとき

$$\alpha, \beta\in\boldsymbol{Z}[i], \beta\neq 0 \text{ ならば},$$
$$\alpha=\beta\gamma+\delta,\quad N(\delta)<N(\beta)$$
$$\text{をみたす } \gamma, \delta\in\boldsymbol{Z}[i] \text{ が存在する}$$

が成り立つ．実際，$\dfrac{\alpha}{\beta}=A+Bi\ (A, B\in\boldsymbol{Q})$とおき，$A, B$に最も近い$a, b\in\boldsymbol{Z}$をえらんで$\gamma=a+bi, \delta=\alpha-\beta\gamma$とすればよい．このとき，$\delta=\beta\left(\dfrac{\alpha}{\beta}-\gamma\right)$から$N(\delta)=N(\beta)N\left(\dfrac{\alpha}{\beta}-\gamma\right)$であるが，$\dfrac{\alpha}{\beta}-\gamma=(A-a)+(B-b)i$とかき，$|A-a|, |B-b|\leqq\dfrac{1}{2}$に注意して$N\left(\dfrac{\alpha}{\beta}-\gamma\right)=(A-a)^2+(B-b)^2<1$となる．したがって，$N(\delta)<N(\beta)$.

$\{a+b\sqrt{2}\mid a, b\in\boldsymbol{Z}\}$では，$\alpha=a+b\sqrt{2}$に対して，$\alpha$のノルムを

$$N(\alpha)=a^2-2b^2$$

ときめる．$0\neq\beta=c+d\sqrt{2}$ならば$\dfrac{\alpha}{\beta}=A+B\sqrt{2}\ \left(A=\dfrac{ac-2bd}{c^2-2d^2},\right.$ $\left.B=\dfrac{bc-ad}{c^2-2d^2}\right)$とおく．$A, B$に最も近い$a, b\in\boldsymbol{Z}$をえらんで$\gamma=a+b\sqrt{2}$，$\delta=\alpha-\beta\gamma$ときめれば，$|N(\delta)|<|N(\beta)|$となって

$$\alpha=\beta\gamma+\delta,\quad |N(\delta)|<|N(\beta)|.$$

例 4 整域Rに対して

$$R[x] \text{ が単項イデアル整域} \Leftrightarrow R \text{ が体}$$

が成り立つ．

$\Rightarrow$: $a\in R, a\neq 0$とし，aがRの単元であることを示す．aとxから生成された$R[x]$のイデアル$(a)+(x)$は単項イデアルであるから，$(a)+(x)=(f(x))$を

みたす 0 でない $f(x)\in R[x]$ が存在する．$a, x\in(f(x))$ から

$$a=f(x)g(x),\quad x=f(x)h(x)$$

とかける．第1式から $f(x)=a_0$ となる R の元 a_0 があり，第2式からは $x=a_0\cdot h(x), h(x)=b_1x$ $(b_1\in R)$ とかける．$x=a_0\cdot b_1x, a_0b_1=1$，したがって，$1\in(a_0)=(f(x))=(a)+(x)$.

$$1=a\cdot k_1(x)+x\cdot k_2(x)$$

$$(k_1(x)=c_0+c_1x+\cdots,\quad k_2(x)=d_0+d_1x+\cdots)$$

とかけば，$1=ac_0+(ac_1+d_0)x+(ac_2+d_1)x^2+\cdots$，$ac_0=1$ で a は R の単元である．

$\Leftarrow$: A を $R[x]$ のイデアルとし，A が単項イデアルであることを示す．$A=\{0\}$ のときは明らか．A が 0 でない R の元 a を含めば，a は R の単元，したがって，$R[x]$ の単元で $A=R[x]$．$A\neq\{0\}$ ではあるが 0 でない R の元を含まないとする．A は 0 でも定数でもない多項式を含むから，その中で次数最小のものを $g(x)$ とする．A の任意の元 $f(x)$ に対して

$$f(x)=g(x)q(x)+r(x),$$

$$r(x)=0 \text{ または } \deg r(x)<\deg g(x)$$

をみたす $q(x), r(x)$ が $R[x]$ に存在する．

$$r(x)=f(x)-g(x)q(x)\in A$$

から，$r(x)$ が定数ならば A の仮定から $r(x)=0$，そうでないときは $g(x)$ の次数の最小性により $r(x)=0$．したがって，$f(x)\in(g(x))$ で $A=(g(x))$ となる．

例 5　例4から $\boldsymbol{Z}[x]$ は単項イデアル整域ではない．例えば，$(2)+(x)$ は単項イデアルではない．

もし $(2)+(x)$ が単項イデアルならば，例4の証明と同じようにして 2 が $\boldsymbol{Z}$ の単元となり矛盾を生ずる．

補題 2.14（因数定理）　K を体，$f(x)\in K[x]$ とする．K の元 a に対して

$$(x-a)\mid f(x) \iff f(a)=0.$$

証明

$$f(x)=(x-a)q(x)+r(x),$$

$$r(x)=0 \text{ または } \deg r(x)<\deg(x-a)=1$$

とかけるが，いずれにせよ $r(x)$ は定数多項式である．x に a を代入して

$$f(a)=(a-a)q(a)+r(x)=r(x).$$

したがって，$r(x)=0 \iff f(a)=0$ となる．

定理 2.15　$f(x)$ が体 K の上の多項式で，次数が n $(\geqq 1)$ ならば，$f(x)$ は K

の中に n 個より多くの根をもちえない．

証明 n に関する帰納法で示す．$n=1$ で

$$f(x)=ax+b \qquad (a\neq 0)$$

のときは，$-a^{-1}b$ がただ1個の根である．

次数 $n-1$ の多項式については定理が正しいとし，$f(x)$ の次数を n とする．$f(x)$ が n 個より多くの根を K の中にもつならば，その1つを c として

$$f(x)=(x-c)g(x)$$

とあらわす．このとき $g(x)$ は次数 $n-1$ の K の上の多項式で，$(n-1)$ 個より多くの根をもち帰納法の仮定に反する．したがって，$f(x)$ は n 個より多くの根をもちえない．

例 6 K を体とし，$f(x), g(x)$ を共に次数 n の $K[x]$ の元とする．もし $(n+1)$ 個の相異なる K の元 $c_1, c_2, \cdots, c_{n+1}$ が存在して

$$f(c_i)=g(c_i) \qquad (1\leqq i\leqq n+1)$$

が成り立つならば，$f(x)$ と $g(x)$ は一致する．

実際，$h(x)=f(x)-g(x)$ は K 上の多項式で，もし0でないならば，その次数は n をこえず，しかも K の中に $(n+1)$ 個の根をもつ．定理2.15から $h(x)$ は定数多項式となるが，これは矛盾．$h(x)=0$ でなければならない．

次の定理は**代数学の基本定理**とよばれる重要な定理であるが，ここではその証明に触れない．巻末の文献 [2], [6] 等をみられたい．

定理 2.16 $f(x)$ が $\boldsymbol{C}$ の上の多項式で，$\deg f(x)\geqq 1$ ならば，$f(x)$ は $\boldsymbol{C}$ の中に少なくとも1個の根をもつ．

一般に，体 K の上の任意の定数でない多項式が K の中に根をもつとき，K を**代数的閉体**とよぶ．$\boldsymbol{C}$ は代数的閉体の最も重要な例である．

例 7 $\boldsymbol{C}$ の上の n 次の多項式 $f(x)$ は

$$f(x)=a\cdot(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) \qquad (a, \alpha_1, \alpha_2, \cdots, \alpha_n\in\boldsymbol{C})$$

と n 個の1次式の積に分解されることを，n に関する帰納法で示す．

$n=1$ のときは明らか．次数 $n-1$ の $\boldsymbol{C}$ の上の多項式については上のことが正しいと仮定し，$f(x)$ を $\boldsymbol{C}$ の上の n 次の多項式とする．定理2.16から $f(x)$ は $\boldsymbol{C}$ に少なくとも1個の根 α_1 をもつ．補題2.14から

$$f(x)=(x-\alpha_1)g(x),$$

$$g(x) \text{ は } \boldsymbol{C} \text{ の上の } (n-1) \text{ 次の多項式}$$

とかける．帰納法の仮定から

$$g(x)=a\cdot(x-\alpha_2)\cdots(x-\alpha_n) \qquad (a, \alpha_2, \cdots, \alpha_n\in \boldsymbol{C})$$

とあらわされるから，

$$f(x)=a\cdot(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$

と1次式の積に分解される．

このとき，$\alpha_1, \alpha_2, \cdots, \alpha_n$ 以外に $f(x)$ は $\boldsymbol{C}$ に根をもたない．実際，β が $\boldsymbol{C}$ における $f(x)$ の根ならば，

$$0=f(\beta)=a\cdot(\beta-\alpha_1)(\beta-\alpha_2)\cdots(\beta-\alpha_n)$$

で，いずれかの i に対して，$\beta-\alpha_i=0$，$\beta=\alpha_i$ となる．

$\boldsymbol{C}$ の上の n 次の多項式 $f(x)$ は

$$f(x)=a\cdot(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) \qquad (a, \alpha_1, \alpha_2, \cdots, \alpha_n\in \boldsymbol{C})$$

の形に分解される．同じ1次式をまとめて

$$f(x)=a\cdot(x-\alpha_{i_1})^{e_1}\cdot(x-\alpha_{i_2})^{e_2}\cdot \cdots \cdot(x-\alpha_{i_m})^{e_m}$$

$(\alpha_{i_1}, \alpha_{i_2}, \cdots, \alpha_{i_m}$ は相異なる $f(x)$ の根，

$e_1, e_2, \cdots, e_m$ は自然数で $e_1+e_2+\cdots+e_m=n)$

とべきの形にかくこともできる．

以上の議論は一般の代数的閉体に対しても成り立つ．したがって，体 K が代数的閉体であるとは

K 上の定数でない多項式がすべて1次式の積に分解される

とのべることもできる（4.3節参照）．

この節の最後に，いわゆる多変数の多項式について触れておこう．

R を可換環とし，x を不定元とする R の上の多項式環 $R[x]$ をつくる．$R[x]$ は可換環であるから，y を不定元とする $R[x]$ の上の多項式環 $(R[x])[y]$ がつくれる．$(R[x])[y]$ の元 g は

$$g=f_0(x)+f_1(x)y+\cdots+f_n(x)y^n$$
$$(f_0(x), f_1(x), \cdots, f_n(x)\in R[x])$$

の形にあらわされる．各 k に対して，$f_k(x)$ を

$$f_k(x)=a_{0k}+a_{1k}x+\cdots+a_{m(k),k}x^{m(k)} \qquad (a_{ik}\in R)$$

とかくならば，g を R の元を係数とする x, y の多項式として

$$g=g(x, y)=\sum_{i=0}^{m(j)}\sum_{j=0}^{n}a_{ij}x^iy^j$$

とかきなおせる．ここで $x^0=y^0=1$ ときめる．

$(R[x])[y]$ を $R[x, y]$ とかき，$R[x, y]$ の元を2つの不定元 x, y に関する R の上の多項式とよぶ．

$R[x, y]$ の2元 $\sum_{i=0}^{m(j)}\sum_{j=0}^{n}a_{ij}x^iy^j$ と $\sum_{i=0}^{m(j)}\sum_{j=0}^{n}b_{ij}x^iy^j$ をとる．ここで必要があれば係数に R の零元 0 をおぎなって，同じ $m(j), n$ を用いてもよい．このとき

$$\sum_i\sum_j a_{ij}x^iy^j=\sum_i\sum_j b_{ij}x^iy^j \Leftrightarrow \text{すべての } i, j \text{ に対して } a_{ij}=b_{ij}$$

であり，和と積を

$$\sum_i\sum_j a_{ij}x^iy^j+\sum_i\sum_j b_{ij}x^iy^j=\sum_i\sum_j (a_{ij}+b_{ij})x^iy^j,$$

$$\sum_i\sum_j a_{ij}x^iy^j\cdot\sum_i\sum_j b_{ij}x^iy^j=\sum_i\sum_j c_{ij}x^iy^j,$$

ただし，

$$c_{ij}=\sum_{\substack{k+k'=i,\\ l+l'=j}} a_{kl}b_{k'l'}$$

ときめて $R[x, y]$ は可換環をつくる．

$R[x, y]$ の 0 でない多項式

$$f(x, y)=\sum_i\sum_j a_{ij}x^ix^j$$

の次数を $a_{ij}\neq 0$ である整数 $i+j$ の最大値ときめ，$\deg f(x, y)$ とかく．定理 2.11 と同じように，R が整域のときには

$$\deg(f(x, y)\cdot g(x, y))=\deg f(x, y)+\deg g(x, y)$$

が成り立つ．

例 8 体 K に対して $K[x]$ は単項イデアル整域であった(例 4)が，このことは $K[x, y]$ では成り立たない．

実際，x, y から生成されたイデアル $(x)+(y)$ は単項イデアルではない．仮りにこれが単項イデアルであるとして

$$(x)+(y)=(f(x, y)) \qquad (f(x, y)\in K[x, y])$$

とおく．$x\in(f(x, y))$ から $f(x, y)\neq 0$ であり，$(x)+(y)=K[x, y]$ とはなりえないから $f(x, y)$ は定数多項式でもない．$x, y\in(f(x, y))$ から

$$x=f(x, y)\cdot k_1(x, y), \quad y=f(x, y)\cdot k_2(x, y)$$

とかく．$\deg x=\deg y=1$ から $\deg f(x, y)=1$ で，したがって，$k_1(x, y), k_2(x, y)$ 共に定数多項式である．

$$k_1(x, y)=a, \quad k_2(x, y)=b \qquad (a, b\in K)$$

$$f(x, y)=c_0+c_1x+c_2y \qquad (c_i\in K)$$

とかけば，

$$x=a\cdot f(x, y)=ac_0+ac_1x+ac_2y,$$

$$y=b\cdot f(x, y)=bc_0+bc_1x+bc_2y.$$

第1式からは $c_2=0$，第2式からは $c_1=0$ をうるが，これは $\deg f(x,y)=1$ に矛盾する．

R の上の n 変数 $x_1, x_2, \cdots, x_n$ の多項式を

$$f(x_1, x_2, \cdots, x_n)=\sum a_{i_1 i_2 \dots i_n} x_1{}^{i_1} x_2{}^{i_2} \cdots x_n{}^{i_n}$$

の形の有限和として定義する．ここで $a_{i_1 i_2 \dots i_n} \in R$ $(i_1, i_2, \cdots, i_n \geqq 0)$ とする．$x_1, x_2, \cdots, x_n$ の多項式の全体も可換環をつくる．この環を $R[x_1, x_2, \cdots, x_n]$ であらわす．$(R[x])[y]=R[x, y]$ と同様

$$R[x_1, x_2, \cdots, x_n]=(R[x_1, x_2, \cdots, x_{n-1}])[x_n]$$

が成り立つ．

2.6 素元分解

整数環 $\boldsymbol{Z}$ では，1より大きい自然数 a は素数の積として

$$a=p_1 p_2 \cdots p_n$$

の形に，因数の順序を除いて，一意的にあらわされる（いわゆる素因数分解ができる）ことはよく知られている．この定理は**整数論の基本定理**とよばれている．この節では，単項イデアル整域においても，同じような定理が成り立つことを証明する．そのために，整数における倍数や約数などの概念を整域にまで広げて次のように定義する．

R を整域とする．$a, b \in R$ に対して $a=bc$ となる $c \in R$ が存在するとき，a を b の**倍元**，b を a の**約元**とよび，$b|a$ とかく．明らかに

$$b|a \iff a \in (b) \iff (a) \subseteqq (b)$$

である．ここで $(a), (b)$ はそれぞれ a, b から生成された R の単項イデアルをあらわす．

$b|a$ でかつ $a|b$ であるとき，すなわち，$(a)=(b)$ のとき，a と b は互いに**同伴**であるといい，$a \sim b$ であらわす．このとき

$$a=bx, \quad b=ay$$

をみたす R の元 x, y が存在するが，$a=bx=ayx$ で $a(1-yx)=0$．$a \neq 0$ のときは $yx=1$ で x は R の単元である．したがって，$a \neq 0$ のとき

$$a \sim b \iff R \text{ の単元 } x \text{ があって } a=bx$$

が成り立つ．

例 1　$\boldsymbol{Z}$ の単元は ± 1 のみであるから，$a, b \in \boldsymbol{Z}$，$a \neq 0$ に対して

$$a \sim b \Leftrightarrow a = \pm b.$$

例 2　体Kの上の多項式環$K[x]$では，単元はKの0でない元にほかならない（2.5節例2）から，$f(x), g(x) \in K[x]$，$f(x) \neq 0$に対して

$$f(x) \sim g(x) \Leftrightarrow K\text{の元 } a \neq 0 \text{ があって } f(x) = a \cdot g(x).$$

$K[x]$の0でない元$f(x)$は

$$\begin{aligned} f(x) &= a_0 + a_1 x + \cdots + a_n x^n \qquad (a_n \neq 0) \\ &= a_n(a_0 a_n^{-1} + a_1 a_n^{-1} x + \cdots + a_{n-1} a_n^{-1} x^{n-1} + x^n) \end{aligned}$$

で，$f_1(x) = a_0 a_n^{-1} + a_1 a_n^{-1} x + \cdots + a_{n-1} a_n^{-1} x^{n-1} + x^n$はモニックな多項式であるから

$$f(x) \sim f_1(x), \quad f_1(x) \text{ はモニック}$$

が成り立つ．

整域Rの0でない元$a_1, a_2, \cdots, a_n$に対して，Rの元dが

(1)　$d | a_i$ $(1 \leqq i \leqq n)$,

(2)　$c \in R$ で $c | a_i$ $(1 \leqq i \leqq n)$ $\Rightarrow$ $c | d$

をみたすとき，dを$a_1, a_2, \cdots, a_n$の**最大公約元**とよぶ．

dが$a_1, a_2, \cdots, a_n$の最大公約元で，$d' \in R$が$d \sim d'$ならば，d'もまた$a_1, a_2, \cdots, a_n$の最大公約元である．したがって，最大公約元は存在しても一意的にはきまらない．しかし，dとd'が共に$a_1, a_2, \cdots, a_n$の最大公約元ならば，条件(2)から$d | d'$かつ$d' | d$で$d \sim d'$をうるから，最大公約元は存在すれば同伴なものしかありえない．

Rの元lが

(1)　$a_i | l$ $(1 \leqq i \leqq n)$,

(2)　$c \in R$ で $a_i | c$ $(1 \leqq i \leqq n)$ $\Rightarrow$ $l | c$

をみたすとき，lを$a_1, a_2, \cdots, a_n$の**最小公倍元**とよぶ．最小公倍元も存在すれば，同伴を除いて一意的である．

例 3　$R = \boldsymbol{Z}$とし，$a_1, a_2, \cdots, a_n$を0でない整数とする．このとき$a_1, a_2, \cdots, a_n$の最大公約数dが存在する（1.5節参照）．dは$a_1, a_2, \cdots, a_n$の公約数であり，$a_1, a_2, \cdots, a_n$の任意の公約数cに対して$d = cq$をみたす整数qが存在した．最大公約数dは(1), (2)の条件をみたし$a_1, a_2, \cdots, a_n$の最大公約元になっている．dと同じように，$-d$も(1), (2)の条件をみたし$a_1, a_2, \cdots, a_n$の最大公約元である．

逆に，d' が $a_1, a_2, \cdots, a_n$ の最大公約元ならば，すぐ上にのべたように $d' \sim d$, $d' = \pm d$ である．

$a_1, a_2, \cdots, a_n$ が 0 でないから $a_1, a_2, \cdots, a_n$ の最小公倍数 l が存在する（1.5 節参照）．このとき $\pm l$ が $a_1, a_2, \cdots, a_n$ の最小公倍元であり，これ以外にはない．この証明は演習問題とする．

定理 2.17　整域 R の 0 でない元 $a_1, a_2, \cdots, a_n$ に対して

$a_1, a_2, \cdots, a_n$ の最大公約元 d があって

$$d = x_1a_1 + x_2a_2 + \cdots + x_na_n \qquad (x_1, x_2, \cdots, x_n \in R)$$

$$\Leftrightarrow\ (a_1) + (a_2) + \cdots + (a_n) \text{ は単項イデアル}$$

が成り立つ．

証明　d が最大公約元ならば，各 i に対して $(a_i) \subseteqq (d)$．したがって，$(a_1) + (a_2) + \cdots + (a_n) \subseteqq (d)$．その上，$d = x_1a_1 + x_2a_2 + \cdots + x_na_n$ とあらわされるならば $d \in (a_1) + (a_2) + \cdots + (a_n)$ で，$(d) = (a_1) + (a_2) + \cdots + (a_n)$ となる．

逆に，$(a_1) + (a_2) + \cdots + (a_n) = (d)$ ならば，各 i に対して，$a_i \in (d)$, $d | a_i$ である．もし $c \in R$, $c | a_i$ $(1 \leqq i \leqq n)$ ならば，上と同じように，$(a_1) + (a_2) + \cdots + (a_n) \subseteqq (c)$ が成り立つから $(d) \subseteqq (c)$．したがって，$c | d$ で d は (1), (2) の条件をみたして $a_1, a_2, \cdots, a_n$ の最大公約元である．このとき，$(d) = (a_1) + (a_2) + \cdots + (a_n)$ から $d = x_1a_1 + x_2a_2 + \cdots + x_na_n$ とあらわされる．

この定理から，R が単項イデアル整域ならば，R の 0 でない元 $a_1, a_2, \cdots, a_n$ に対して最大公約元 d が存在して

$$(d) = (a_1) + (a_2) + \cdots + (a_n)$$

が成り立つ．

R を整域とする．どんな R の元 a も適当な R の元 b, c をみつけて，$a = bc$ とかくことができる．例えば，$a = a \cdot 1$ であり，単元 b を用いて $a = b \cdot (b^{-1}a)$ ともできる．この例のように，1 つの因子が単元であるような分解を**自明な分解**とよぶ．0 でも単元でもない R の元 p が自明な分解しかもたないとき，すなわち，

$$p = ab \ \Rightarrow\ a \text{ または } b \text{ が単元}$$

のとき，p を R の**素元**とよぶ．

例 4　$\boldsymbol{Z}$ の素元は $\pm p$（p は素数）である．この証明は演習問題とする．

整域Rの上の多項式$f(x)$が定数多項式ではないとする．このとき，定数でない多項式$g(x), h(x)$が$R[x]$にあって

$$f(x)=g(x)h(x)$$

の形に分解されるならば，$f(x)$を$R[x]$の**可約多項式**，そうでないならば，$f(x)$を$R[x]$の**既約多項式**とよぶ．

例 5　Kを体とし，$K[x]\ni f(x)$とする．$f(x)$が0でないときは

$$f(x)\text{ が } K[x] \text{ の単元} \Leftrightarrow \deg f(x)=0$$

であるから，$f(x)$が$K[x]$の素元とは

(1)　$\deg f(x)>0$,

(2)　$f(x)=g(x)h(x) \quad (g(x), h(x)\in K[x])$

$\Rightarrow \deg g(x)=0$ または $\deg h(x)=0$

を意味する．このことは，$f(x)$が$K[x]$の既約多項式にほかならないことを示している．

例 6　体Kの上の1次式$f(x)=ax+b$は$K[x]$の素元である．

多項式が既約であるか，可約であるかは係数環に依存する．1つの多項式がある整域の上の多項式とみては既約であり，別な整域の上の多項式とみては可約であるということがよくある．

例 7

$$f(x)=x^2+1$$

は$\boldsymbol{R}[x]$の既約多項式ではあるが，$\boldsymbol{C}[x]$では

$$f(x)=(x+i)(x-i)$$

と分解される．$\boldsymbol{Z}/(2)$の上の多項式とみても

$$f(x)=(x+\bar{1})(x+\bar{1})$$

と分解されて可約な多項式である．

例 8　$\boldsymbol{Z}/(2)$の上では，$f(x)=x^3+x+\bar{1}$は既約である．

もし$f(x)$が可約ならば，$f(x)$は$\boldsymbol{Z}/(2)$の上の次数1の多項式で割り切れる．補題2.14から$\boldsymbol{Z}/(2)$の元$\bar{0}, \bar{1}$を$f(x)$のxに代入して

$$f(\bar{0})=\bar{0} \text{ または } f(\bar{1})=\bar{0}$$

となるはずである．しかし，

$$f(\bar{0})=f(\bar{1})=\bar{1}$$

で矛盾である．

このように体Kが有限集合のときは，その可能な根を代入して，既約かどうかを確かめられる場合がある．

例 9　$f(x)=x^2-2$ は $\boldsymbol{R}$ の上の多項式とみれば,

$$x^2-2=(x+\sqrt{2})(x-\sqrt{2})$$

と可約であるが, $\boldsymbol{Q}$ の上の多項式とみれば既約である.

もし $\boldsymbol{Q}$ の上の多項式とみて可約ならば, 適当な $\boldsymbol{Q}$ の元 a, b, c, d に対して

$$x^2-2=(ax+b)(cx+d)$$

と分解される. したがって,

$$ac=1, \quad ad+bc=0, \quad bd=-2.$$

$a\neq 0$, $b\neq 0$ であり, $c=\dfrac{1}{a}$, $d=-\dfrac{2}{b}$ を $ad+bc=0$ に代入して

$$-\frac{2a}{b}+\frac{b}{a}=0, \quad -2a^2+b^2=0.$$

これから $\left(\dfrac{b}{a}\right)^2=2$ となるが, $\sqrt{2}$ は有理数でないから矛盾である.

極大イデアルの概念 (2.3 節例12) を用いて, 素元を特徴づけることができる.

補題 2.18　R が整域で, p は 0 でも単元でもない R の元とする. このとき,

(1)　$p|ab\ (a, b\in R) \Rightarrow p|a$ または $p|b$,

(2)　$p=ab\ (a, b\in R) \Rightarrow a$ または b は R の単元,

(3)　p から生成された単項イデアル (p) は R の極大イデアル

で, (1) ⇒ (2) であり, (3) ⇒ (1) である.

特に, R が単項イデアル整域ならば, (2) ⇒ (3)でもあって, すべての条件が同値となる.

証明　(1) ⇒ (2): $p=ab$ とする. $p|ab$ であるから $p|a$ または $p|b$ である. $p|a$ ならば $a=px=(ab)x$ をみたす R の元 x がある. $a\neq 0$ であるから $bx=1$ で b は単元である. $p|b$ のときは a が単元である.

(3) ⇒ (1): $p|ab$ で $p\nmid a$ とする. このとき $(p)\subsetneqq(p)+(a)$ であるから $R=(p)+(a)$. したがって, $1=px+ay$ をみたす R の元 x, y が存在し, $b=pbx+aby\in(p)$ で $p|b$ となる.

(2) ⇒ (3): R を単項イデアル整域とし, (2) を仮定して (p) が極大イデアルであることを示す. (p) を含む R のイデアルを (a) とかく. $p\in(a)$ で $p=ab$ となる R の元 b がある. (2)から a または b は単元である. a が単元のときは $(a)=R$ であり, b が単元のときは $a=pb^{-1}$ で $(a)\subseteqq(p)$ となり, $(a)=(p)$ をうる. したがって, (p) は極大イデアルである.

一般に，可換環RのイデアルAが$a, b\in R$に対して

$$ab\in A \Rightarrow a\in A \text{ または } b\in A$$

をみたすとき，AをRの**素イデアル**とよぶ．

補題2.18の条件(1)は(p)が素イデアルであることを，(3) ⇒ (1)の証明は極大イデアルはいつも素イデアルであることを示している．補題2.18はRが単項イデアル整域ならば，次の3つの概念が同じであることを示している．

(1) (p)が素イデアル．

(2) pが素元．

(3) (p)が極大イデアル．

整域Rの0でも単元でもない任意の元が素元の積として．順序と単元因子のちがいを除いて一意的にあらわされるとき，すなわち，

(1) Rの0でも単元でもない元aは

$$a=p_1p_2\cdots p_n$$

と素元$p_1, p_2, \cdots, p_n$の積としてあらわされる，

(2) $a=p_1p_2\cdots p_n=q_1q_2\cdots q_m$と素元の積として二通りにあらわされるならば，$n=m$で，適当に番号をつけかえて

$$p_1\sim q_1, p_2\sim q_2, \cdots, p_n\sim q_n$$

とできる

とき，Rを**一意分解整域**とよぶ．この分解で同じ素元をまとめて

$$a=p_1^{e_1}p_2^{e_2}\cdots p_m^{e_m}$$

$$(p_1, p_2, \cdots, p_m \text{ は相異なる素元，} e_1, e_2, \cdots, e_m \text{ は自然数})$$

とべきの形であらわすこともできる．

整数論の基本定理を拡張して，次の定理が成り立つ．

定理 2.19 単項イデアル整域Rは一意分解整域である．

証明 0でも単元でもないRの元で素元の積にあらわされないものがあったとする（ここで素元自身も素元の積とみる）．その1つをa_1とする．a_1は素元でないから$a_1=bc$という自明でない分解をもつ．ここでb, c共に素元の積ならば，a_1が素元の積となるからb, cのいずれかは素元の積にあらわされない．それをbとして$b=a_2$とおく．

a_2は0でも単元でもないRの元で素元の積にあらわされないから，a_1と全く同じ仮定をみたす．その上，cも単元でないから，a_1とa_2とは同伴でない．したがって，$(a_1)\subsetneqq(a_2)$となる．

次に，a_1 のかわりに a_2 に対して同じ議論をおこなう．これをくりかえせば

$$(a_1)\subsetneqq(a_2)\subsetneqq(a_3)\subsetneqq\cdots$$

という単項イデアルの無限列ができる．これが矛盾であることは次の補題から分かる．

補題 2.20　単項イデアル整域 R の 0 でない元の列 $a_1, a_2, \cdots$ に対して，

$$(a_1)\subseteqq(a_2)\subseteqq\cdots \Rightarrow \text{ある } n \text{ があって } (a_n)=(a_{n+1})=\cdots$$

が成り立つ．

証明　$(a_1)\subseteqq(a_2)\subseteqq\cdots$ とする．イデアル (a_i) すべての和集合 $\bigcup(a_i)$ はイデアルをつくり（演習問題 53），R が単項イデアル整域であるから，$\bigcup(a_i)=(d)$ をみたす R の元 d が存在する．

$$(a_1)\subseteqq(a_2)\subseteqq\cdots\subseteqq\bigcup(a_i)=(d).$$

このとき，ある n があって $d\in(a_n)$．したがって，$(d)\subseteqq(a_n)$．$(d)=(a_n)$ で $(a_n)=(a_{n+1})=\cdots$ となる．

定理 2.19 の証明にもどって，一意性を示す．a が

$$a=p_1p_2\cdots p_n=q_1q_2\cdots q_m \qquad (p_i, q_j \text{ は素元})$$

と二通りにあらわされたとする．$p_1|q_1q_2\cdots q_m$ から $p_1|q_i$ なる q_i が存在する（補題 2.18）．必要ならば番号をつけかえて，これを q_1 とする．$q_1=p_1u_1$ とかけば，q_1 は素元であるから u_1 は R の単元である．したがって $p_1\sim q_1$．$q_1=p_1u_1$ をもとの式に代入して

$$p_1p_2\cdots p_n=u_1p_1q_2\cdots q_m.$$

$p_1(p_2\cdots p_n)=p_1(u_1q_2\cdots q_m)$ から

$$p_2p_3\cdots p_n=u_1q_2q_3\cdots q_m.$$

p_2 は $u_1, q_2, \cdots, q_m$ のいずれかを割るが，p_2 が単元 u_1 を割ることはない（演習問題 50）から，$p_2|q_j$，$2\leqq j\leqq m$ となる．必要ならば番号をつけかえて，これを q_2 とすれば，上と同じようにして

$$p_3p_4\cdots p_n=u_1u_2q_3\cdots q_m \qquad (u_2 \text{ は } R \text{ の単元})$$

であり，かつ $p_2\sim q_2$ をうる．これをくりかえしていけば，

$$n\leqq m \text{ で，} p_1\sim q_1, p_2\sim q_2, \cdots, p_n\sim q_n$$

となる．もし $n<m$ ならば

$$1=u_1u_2\cdots u_nq_{n+1}\cdots q_m$$

であるが，これは例えば，q_{n+1} が単元となって矛盾である．したがって，

$$n=m, p_1\sim q_1, p_2\sim q_2, \cdots, p_n\sim q_n.$$

例 10　体 K に対して，2.5 節例 3 から，$K[x]$ は一意分解整域である．

したがって，0でも定数でもないKの上の多項式$f(x)$は

$$f(x)=p_1(x)p_2(x)\cdots p_n(x) \qquad (p_i(x)\text{ は既約多項式})$$

の形に，$p_i(x)$の順序と0でない定数因子のちがいを除いて，一意的にあらわされる．

各$p_i(x)$を最高次係数でくくって

$$p_i(x)=a_i\cdot p_i'(x) \qquad (p_i'(x)\text{ はモニック})$$

とかけば，$f(x)$を

$$f(x)=a\cdot p_1'(x)\,p_2'(x)\cdots p_n'(x) \qquad (a=a_1a_2\cdots a_n)$$

とモニックな既約多項式の積の形に分解することができる．モニックな2つの多項式$h(x), k(x)$では

$$h(x)\sim k(x) \Leftrightarrow h(x)=k(x)$$

を意味するから，この分解は$p_i'(x)$の順序のみを除いて一意的である．

特に，$\boldsymbol{C}$の上のn次の多項式$f(x)$は

$$f(x)=a\cdot(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) \qquad (a, \alpha_1, \alpha_2, \cdots, \alpha_n\in\boldsymbol{C})$$

とn個の1次式の積に分解される（2.5節例6）から，$\boldsymbol{C}$の上の既約多項式とは1次式にほかならない．

この分解は$f(x)$のモニックな既約多項式への分解であり，同じ1次式をまとめて

$$f(x)=a\cdot(x-\alpha_1)^{e_1}\cdot(x-\alpha_2)^{e_2}\cdot\cdots\cdot(x-\alpha_m)^{e_m}$$
$$(\alpha_1, \alpha_2, \cdots, \alpha_m\text{ は相異なる }\boldsymbol{C}\text{ の元，}$$
$$e_1, e_2, \cdots, e_m\text{ は自然数で }e_1+e_2+\cdots+e_m=n)$$

のようにかくこともできる．

例 11　$\boldsymbol{C}$の場合とちがって，$\boldsymbol{R}$の上の多項式では，既約多項式は1次式にかぎらない．例えば，x^2+1は$\boldsymbol{R}$の上で既約であった．

一般に，$\boldsymbol{R}$の上の2次式$f(x)$が既約である必要十分条件は，$f(x)$が虚根をもつことである．このとき，その1つの根を$\alpha=a+bi$ $(a, b\in\boldsymbol{R}, b\neq 0)$とかけば，他の根は$\bar{\alpha}=a-bi$であるから，ある$c\in\boldsymbol{R}$があって

$$\begin{aligned}f(x)&=c\cdot(x-(a+bi))(x-(a-bi))\\&=c\cdot(x^2-2ax+(a^2+b^2))\end{aligned}$$

とあらわされる．

定理 2.21　$f(x)$が$\boldsymbol{R}$の上の多項式で，$\deg f(x)\geqq 1$ならば，$f(x)$は1次式か$x^2-2ax+(a^2+b^2)$ $(b\neq 0)$の形の2次式の積に分解される．特に，

$f(x)$ が $\boldsymbol{R}$ の上で既約 $\Leftrightarrow$ $f(x)$ は1次式か

$x^2-2ax+(a^2+b^2)$ $(b \neq 0)$ の形の2次式.

証明　$f(x)$ を n 次の $\boldsymbol{R}$ の上の多項式とする．これを $\boldsymbol{C}$ の上の多項式とみて

$$f(x)=a\cdot(x-\alpha_1)^{e_1}\cdot(x-\alpha_2)^{e_2}\cdot\ \cdots\ \cdot(x-\alpha_m)^{e_m}$$

$$(a\in\boldsymbol{R},\ \ \alpha_1,\alpha_2,\cdots,\alpha_m \text{ は相異なる } \boldsymbol{C} \text{ の元},$$

$$e_1,e_2,\cdots,e_m \text{ は自然数で } e_1+e_2+\cdots+e_m=n)$$

と分解する．写像

$$\boldsymbol{C}[x]\to\boldsymbol{C}[x],\quad f(x)\to\bar{f}(x)$$

は環同型である(演習問題55)から

$$\bar{f}(x)=a\cdot(x-\bar{\alpha}_1)^{e_1}\cdot(x-\bar{\alpha}_2)^{e_2}\cdot\ \cdots\ \cdot(x-\bar{\alpha}_m)^{e_m}$$

が成り立つ.

$f(x)$ は $\boldsymbol{R}$ の上の多項式であるから，$f(x)=\bar{f}(x)$ であり，$\{\alpha_1,\alpha_2,\cdots,\alpha_m\}$ は $f(x)$ の相異なる根の全体で，$\{\bar{\alpha}_1,\bar{\alpha}_2,\cdots,\bar{\alpha}_m\}$ は $\bar{f}(x)$ の相異なる根の全体であるから

$$\{\alpha_1,\alpha_2,\cdots,\alpha_m\}=\{\bar{\alpha}_1,\bar{\alpha}_2,\cdots,\bar{\alpha}_m\}.$$

必要ならば番号をつけかえて

$$\alpha_1,\alpha_2,\cdots,\alpha_s\notin\boldsymbol{R},\quad \alpha_{s+1},\cdots,\alpha_m\in\boldsymbol{R}$$

とすると，$\bar{\alpha}_{s+1}=\alpha_{s+1},\cdots,\bar{\alpha}_m=\alpha_m$ であるから

$$\{\alpha_1,\alpha_2,\cdots,\alpha_s\}=\{\bar{\alpha}_1,\bar{\alpha}_2,\cdots,\bar{\alpha}_s\}.$$

したがって，各 α_i $(1\leqq i\leqq s)$ はいずれかの $\bar{\alpha}_j$ $(1\leqq j\leqq s)$ と一致し，その上，$i\neq j$ である．$\alpha_i=\bar{\alpha}_j$ であるとき，i,j を対 (i,j) として考える．$\alpha_i=\bar{\alpha}_j$ から $\bar{\alpha}_i=\alpha_j$ が成り立つから，(i,j) が対ならば (j,i) も対をつくる.

対をつくる (i,j) に対して α_i,α_j を $\{\alpha_1,\alpha_2,\cdots,\alpha_s\}$ から次々にとり去る．も

$\dfrac{f(x)}{(x-\alpha_i)^{e_i}}$ は $x-\alpha_i$ を因子にもたないが，$\dfrac{\bar{f}(x)}{(x-\alpha_i)^{e_i}}=\dfrac{\bar{f}(x)}{(x-\bar{\alpha}_j)^{e_i}}$ は $x-\bar{\alpha}_j$ $=x-\alpha_i$ を因子にもって矛盾を生ずる．$e_i>e_j$ のときも同様で，したがって，$e_i=e_j$ である.

(i,j) が対をつくっているとき，

$$\alpha_i=a+bi\qquad(a,b\in\boldsymbol{R},\ \ b\neq 0)$$

とかけば，$\alpha_j=\bar{\alpha}_i=a-bi$ であり，$e_i=e_j$ であるから積

し s が奇数ならば，対をつくらない k $(1\leqq k\leqq s)$ が1個残る．このとき，$\alpha_k=\bar{\alpha}_k$ が成り立ち，$\alpha_k\notin\boldsymbol{R}$ に矛盾する．s は偶数でなければならない.

その上，対 (i,j) に対して $e_i=e_j$ である．実際，$e_i<e_j$ であるならば

$$(x-\alpha_i)^{e_i}\cdot(x-\alpha_j)^{e_j}=\{(x-(a+bi))(x-(a-bi))\}^{e_i}$$
$$=(x^2-2ax+(a^2+b^2))^{e_i}$$

は $\boldsymbol{R}$ の上の多項式となる．結局，$f(x)$ は

$$f(x)=a\cdot(x-\alpha_1)^{e_1}\cdot\cdots\cdot(x-\alpha_s)^{e_s}\cdot(x-\alpha_{s+1})^{e_{s+1}}\cdot\cdots\cdot(x-\alpha_m)^{e_m}$$
$$=a\cdot(x-2ax+(a^2+b^2))^{e_1}\cdot\cdots\cdot(x-\alpha_{s+1})^{e_{s+1}}\cdot\cdots$$

の形に分解される．

例 12　$\boldsymbol{R}$ の上の多項式 $f(x)=x^3+1$ はよく知られているように

$$f(x)=(x+1)(x^2-x+1)$$

と $\boldsymbol{R}$ の上の 1 次式と 2 次式の積に分解される．$a=\dfrac{1}{2}$，$b=\dfrac{\sqrt{3}}{2}$ にとれば，

$$x^2-x+1=x^2-2ax+(a^2+b^2)$$

の形をもつ．

$f(x)=x^4+1$ は $\boldsymbol{R}$ の上の 1 次式では割り切れない．2 次の因数を求めるために，$f(x)$ を $\boldsymbol{C}$ の上の多項式とみて 1 次式の積に分解する．

$x^4+1=(x^2-i)(x^2+i)$ で，$x^2-i=0$ をみたす x を求めるために $x=a+bi$ $(a, b\in\boldsymbol{R})$ とおけば，$a=b=\pm\dfrac{1}{\sqrt{2}}$ から $x=\dfrac{1+i}{\sqrt{2}}$ または $x=\dfrac{-1-i}{\sqrt{2}}$ をうる．このxを α_1, α_2 とおく．同じように $x^2+i=0$ をみたす x を求めるために，$x=c+di$ $(c, d\in\boldsymbol{R})$ とおけば，$c=-d=\pm\dfrac{1}{\sqrt{2}}$ から $x=\dfrac{1-i}{\sqrt{2}}$ または $x=\dfrac{-1+i}{\sqrt{2}}$ をうる．この x を α_3, α_4 とおく．したがって，$f(x)$ は

$$x^4+1=\left(x-\frac{1+i}{\sqrt{2}}\right)\left(x-\frac{-1-i}{\sqrt{2}}\right)\left(x-\frac{1-i}{\sqrt{2}}\right)\left(x-\frac{-1+i}{\sqrt{2}}\right)$$

と $\boldsymbol{C}$ の上の 1 次式の積に分解される．

α_i はすべて $\boldsymbol{R}$ の元ではなく，$\{1, 3\}$, $\{2, 4\}$ と対をつくり

$$(x-\alpha_1)(x-\alpha_3)=x^2-\sqrt{2}x+1$$
$$(x-\alpha_2)(x-\alpha_4)=x^2+\sqrt{2}x+1$$

であるから

$$x^4+1=(x^2-\sqrt{2}x+1)(x^2+\sqrt{2}x+1)$$

と $\boldsymbol{R}$ の上の 2 次式の積に分解される．

$\boldsymbol{C}$ とか $\boldsymbol{R}$ の上の多項式が既約であるかどうかはすぐ分かる．これに対して，$\boldsymbol{Z}$ とか $\boldsymbol{Q}$ の上の多項式が既約であるかどうかの判定は容易ではない．ここでは，$f(x)\in\boldsymbol{Z}[x]$ に対して

$$f(x) \text{ が } \boldsymbol{Z} \text{ の上で既約} \Leftrightarrow f(x) \text{ が } \boldsymbol{Q} \text{ の上で既約}$$

であることを，もっと一般的にのべる．$\Leftarrow$ は明らかであるが，$\Rightarrow$ を示すには準備が必要である．

Rを一意分解整域とし，Rの上の 0 でない多項式でその係数の共通な約元がRの単元のみであるものを**原始多項式**とよぶ．

$$f(x)=a_0+a_1x+\cdots+a_nx^n$$

をRの上の多項式とし，$a_0, a_1, \cdots, a_n$ の中で 0 でないものの最大公約元を d とおく．

$$a_i=da_i' \quad (1\leqq i\leqq n), \quad f_1(x)=a_0'+a_1'x+\cdots+a_n'x^n$$

とかけば，

$$f(x)=d\cdot f_1(x), \quad f_1(x) \text{ は原始多項式}$$

となる．

ここで 0 でないRの元 a, b に対して，a, b のいずれかが，例えば，a が単元ならば a, b の最大公約元は a であり，a も b も単元でないときは

$$a=p_1^{e_1}p_2^{e_2}\cdots p_n^{e_n}, \quad b=p_1^{f_1}p_2^{f_2}\cdots p_n^{f_n}$$

$$(p_1, p_2, \cdots, p_n \text{ は相異なる } R \text{ の素元，} e_i, f_j \text{ は整数で } e_i\geqq 0, f_j\geqq 0)$$

とあらわせば，a, b の最大公約元は

$$p_1^{m_1}p_2^{m_2}\cdots p_n^{m_n} \qquad (m_i=\min\{e_i, f_i\})$$

で与えられる．この証明は演習問題とする．2個以上のRの元の最大公約元も同じように求めることができる．

補題 2.22（ガウスの補題） 原始多項式の積は原始多項式である．

証明

$$f(x)=a_0+a_1x+\cdots+a_nx^n \qquad (a_n\neq 0),$$
$$g(x)=b_0+b_1x+\cdots+b_mx^m \qquad (b_m\neq 0)$$

は共に原始多項式で，積

$$f(x)g(x)=c_0+c_1x+\cdots+c_{n+m}x^{n+m}$$

は原始多項式ではないとする．単元でないRの元 d があって

$$d\,|\,c_0, c_1, \cdots, c_{n+m}.$$

d は 0 でも単元でもないから素元の積に分解できる．したがって，Rの素元で $c_0, c_1, \cdots, c_{n+m}$ の共通の約元となるものがある．それを p とおく．p は単元でないから

$$p\,|\,a_0, a_1, \cdots, a_{s-1}, \quad p\nmid a_s,$$
$$p\,|\,b_0, b_1, \cdots, b_{t-1}, \quad p\nmid b_t$$

をみたす番号 s と t がある．このとき

$$a_sb_t=c_{s+t}-(a_0b_{s+t}+a_1b_{s+t-1}+\cdots+a_{s-1}b_{t+1}+a_{s+1}b_{t-1}+\cdots+a_{s+t}b_0)$$

であるから $p|a_sb_t$. したがって, $p|a_s$ または $p|b_t$ となって矛盾である.

R を一意分解整域, M をその商体とし, $R\subseteqq M$ とみる. このとき $f(x)\in R[x]$ をそのまま $f(x)\in M[x]$ とみることができる.

補題 2.23 $f_1(x), f_2(x)\in R[x]$ を共に原始多項式とする. このとき,

$$M[x] \text{ で } f_1(x)\sim f_2(x) \Rightarrow R[x] \text{ で } f_1(x)\sim f_2(x).$$

証明 $M[x]$ で $f_1(x)\sim f_2(x)$ ならば, $f_1(x)=ab^{-1}\cdot f_2(x)$ をみたす 0 でない M の元 ab^{-1} が存在する. $b\cdot f_1(x)=a\cdot f_2(x)$ であり, $b\cdot f_1(x)$ の 0 でない係数の最大公約元を d として

$$b\cdot f_1(x)=d\cdot f_1'(x) \qquad (f_1'(x)\in R[x])$$

とかく. b は $b\cdot f_1(x)$ の係数の共通な約元であるから, $b|d, d=bu$ をみたす R の元 u がとれる. このとき

$$b\cdot(f_1(x)-u\cdot f_1'(x))=0$$

で, $b\neq 0$, $R[x]$ は整域であるから

$$f_1(x)-u\cdot f_1'(x)=0, \quad f_1(x)=u\cdot f_1'(x).$$

この式から u が $f_1(x)$ の係数の共通な約元であることが分かるが, $f_1(x)$ は原始多項式であるから u は R の単元でなければならない.

$b\cdot f_1(x)=a\cdot f_2(x)$ で $a\neq 0$ であるから, 上と同じようにして

$$d=au' \qquad (u' \text{ は } R \text{ の単元})$$

となる. したがって, $bu=d=au', a=buu'^{-1}$ で

$$b\cdot f_1(x)=a\cdot f_2(x)=buu'^{-1}\cdot f_2(x),$$

$$b\cdot(f_1(x)-uu'^{-1}\cdot f_2(x))=0$$

となり, $f_1(x)=uu'^{-1}f_2(x)$ をうる. これは $R[x]$ で $f_1(x)\sim f_2(x)$ を意味している.

補題 2.24 R を一意分解整域とし, その商体を M, $R\subseteqq M$ とみる. このとき

(1) $M[x]\ni f(x)\neq 0$ は

$$f(x)=\varepsilon\cdot f_1(x)$$

のように M の元 ε と R の上の原始多項式 $f_1(x)$ の積としてあらわされる.

(2) この分解において, $\varepsilon, f_1(x)$ は R の単元を除いて一意的にきまる.

証明 (1) $M[x]\ni f(x)\neq 0$ を

$$f(x)=a_0b_0^{-1}+a_1b_1^{-1}x+\cdots+a_nb_n^{-1}x^n$$

とかく. a_i, b_i $(1\leqq i\leqq n)$ は R の元である. $(b_0b_1\cdots b_n)^{-1}\in M$ であり, これでく

くって

$$f(x)=(b_0b_1\cdots b_n)^{-1}\cdot f'(x) \qquad (f'(x)\in R[x])$$

とかく.

$f'(x)$ の 0 でない係数の最大公約元を d として

$$f'(x)=d\cdot f_1(x) \qquad (f_1(x)\text{ は原始多項式})$$

とかけば, $f(x)=(b_0b_1\cdots b_n)^{-1}d\cdot f_1(x)$ となる.

(2)
$$f(x)=\varepsilon_1\cdot f_1(x)=\varepsilon_2\cdot f_2(x)$$
$$(\varepsilon_1, \varepsilon_2\in M,\ f_1(x), f_2(x)\text{ は原始多項式})$$

と分解されたとする. このとき, $f_1(x)=\varepsilon_1^{-1}\varepsilon_2\cdot f_2(x)$ で

$$M[x]\text{ で }f_1(x)\sim f_2(x).$$

補題 2.23 から $R[x]$ で $f_1(x)\sim f_2(x)$. すなわち, R の単元 u があって

$$f_1(x)=u\cdot f_2(x).$$

したがって, $\varepsilon_2\cdot f_2(x)=\varepsilon_1\cdot f_1(x)=\varepsilon_1 u\cdot f_2(x)$, $(\varepsilon_2-\varepsilon_1 u)\cdot f_2(x)=0$ となる. $f_2(x)\neq 0$, $R[x]$ は整域であるから, $\varepsilon_2=\varepsilon_1 u$.

R を一意分解整域とし, その商体を M, $R\subseteq M$ とみる. $M[x]\ni f(x)\neq 0$ が

$$f(x)=g(x)\,h(x) \qquad (g(x), h(x)\in M[x])$$

と分解されたとする. 補題 2.24 から

$$f(x)=\varepsilon_1\cdot f_1(x) \qquad (\varepsilon_1\in M,\ f_1(x)\text{ は原始多項式}),$$
$$g(x)=\varepsilon_2\cdot g_1(x) \qquad (\varepsilon_2\in M,\ g_1(x)\text{ は原始多項式}),$$
$$h(x)=\varepsilon_3\cdot h_1(x) \qquad (\varepsilon_3\in M,\ h_1(x)\text{ は原始多項式})$$

とあらわせば,

$$\varepsilon_1\cdot f_1(x)=\varepsilon_2\varepsilon_3\cdot g_1(x)h_1(x)$$

補題 2.24 の証明から, R の単元 u があって

$$\varepsilon_1 u=\varepsilon_2\varepsilon_3, \quad f_1(x)=u\cdot g_1(x)h_1(x).$$

したがって, $R[x]$ において $f_1(x)\sim g_1(x)h_1(x)$ であり, M において $\varepsilon_1\sim\varepsilon_2\varepsilon_3$ である.

もともと $f(x)\in R[x]$ ならば, $\varepsilon_1\in R$ であり

$$f(x)=\varepsilon_1\cdot f_1(x)=\varepsilon_1 u\cdot g_1(x)h_1(x)$$

であるから, $f(x)$ は 2 つの R の上の多項式 $\varepsilon_1 u\cdot g_1(x)$ と $h_1(x)$ の積に分解される. すなわち,

定理 2.25　R を一意分解整域, その商体を M とする. R の上の 0 でない多項式 $f(x)$ に対して

$$f(x) \text{ が} M \text{で可約} \Leftrightarrow f(x) \text{ は} R \text{で可約}.$$

例 13　$\boldsymbol{Z}$ の上の多項式 $f(x)=x^4-x-3$ は $\boldsymbol{Q}$ の上で既約である．

実際，もし $\boldsymbol{Q}$ で可約とすると，$f(x)$ は $\boldsymbol{Q}[x]$ において 1 次または 2 次の因子をもつ．定理 2.25 から $f(x)$ は $\boldsymbol{Z}[x]$ に 1 次または 2 次の因子をもつ．

$ax+b$ を $f(x)$ の $\boldsymbol{Z}[x]$ における 1 次の因子とすると

$$f(x)=(ax+b)(cx^3+\cdots+d)$$

と分解され，係数を比較して $a|1, b|3$ であるから

$$a=\pm 1, \quad b=\pm 1 \text{ または } \pm 3$$

となる．

$a=\pm 1$ から $\pm b$ は $f(x)$ の根であるが，

$$f(\pm 1)\neq 0, \quad f(\pm 3)\neq 0$$

でこれは矛盾．したがって，$f(x)$ は $\boldsymbol{Z}[x]$ で 1 次の因子をもたない．

$f(x)$ が $\boldsymbol{Z}[x]$ で 2 次の因子をもつとすると，それは

$$x^2-ax\pm 1, \quad x^2-ax\pm 3$$

のいずれかの形をしている．しかし，もし $f(x)$ が

$$f(x)=(x^2-ax-1)h(x) \qquad (h(x)\in \boldsymbol{Z}[x])$$

とかけるならば，$-1=f(-1)=a\cdot h(-1)$ であるから $a=\pm 1$ である．$a=1$ ならば $f(x)=(x^2-x-1)h(x)$ で，このとき $81=f(-3)=11\cdot h(3)$ でこれは矛盾．$a=-1$ ならば $f(x)=(x^2+x-1)h(x)$ で，このとき $11=f(2)=5\cdot h(2)$ でこれも矛盾である．

x^2-ax+1，$x^2-ax\pm 3$ の形の因子をもちえないことも同じように確かめることができる．詳しい証明は演習問題とする．

R が一意分解整域ならば，R の上の多項式環 $R[x]$ もまた一意分解整域であるが，ここではその証明には触れない．この事実から，定理 2.19 の逆が成り立たないことのみ注意しておく．実際，$\boldsymbol{Z}$ は一意分解整域であるから $\boldsymbol{Z}[x]$ も一意分解整域であるが，$\boldsymbol{Z}[x]$ は単項イデアル整域ではなかった (2.5 節例 3)．

次の定理は多項式が既約かどうかの判定にしばしば利用され，**アイゼンシュタインの規準**とよばれている．定理をのべる前に**二項定理**に触れる．

可換環 R の任意の元 a, b と任意の自然数 n とに対して

$$(a+b)^n=\sum_{i=0}^{n} {}_n\mathrm{C}_i\, a^{n-i}b^i$$

が成り立つ（この証明は演習問題とする）．ここで ${}_n\mathrm{C}_i$ は二項係数 $\dfrac{n!}{i!(n-i)!}$ をあらわす．

特に，n が素数 p のときは

$$ {}_p\mathrm{C}_1,\ {}_p\mathrm{C}_2,\ \cdots,\ {}_p\mathrm{C}_{p-1} $$

がすべて p で割り切れることを示す．

$m={}_p\mathrm{C}_i\ (1\leqq i\leqq p-1)$ とおく．

$$ p\cdot(p-1)!=p!=m\cdot i!(p-i)! $$

から $p|m\cdot i!(p-i)!$ であるが，p と $i!$，p と $(p-i)!$ とはそれぞれ互いに素であるから $p|m$ でなければならない．

定理 2.26　Rを一意分解整域，Mをその商体とする．

$$ f(x)=a_0+a_1x+\cdots+a_nx^n $$

をRの上の定数でない多項式とし，Rの素元pで

(1)　$p\nmid a_n$,

(2)　$p\,|\,a_0, a_1, \cdots, a_{n-1}$,

(3)　$p^2\nmid a_0$

をみたすものがあれば，$f(x)$ はMにおいて既約である．

証明　$f(x)$ がMで可約とすると，Rでも可約であるから

$$ f(x)=g(x)h(x)\qquad(\deg g(x), \deg h(x)\geqq 1) $$

をみたすRの上の多項式 $g(x), h(x)$ が存在する．

$$ g(x)=b_0+b_1x+\cdots+b_mx^m,\quad h(x)=c_0+c_1x+\cdots+c_lx^l $$

とかけば，$b_0c_0=a_0, p|a_0, p^2\nmid a_0$ であるから p は b_0 か c_0 のいずれか一方のみを割り切る．仮に $p|b_0, p\nmid c_0$ とする．p が $b_1, b_2, \cdots, b_m$ のすべてを割り切れば，$p|a_n$ となるから

$$ p|b_0, b_1, \cdots, b_{r-1},\ \ p\nmid b_r\qquad(0\leqq r\leqq m<n) $$

をみたす r がある．このとき $f(x)$ の x^r の係数は

$$ a_r=b_0c_r+b_1c_{r-1}+\cdots+b_{r-1}c_1+b_rc_0 $$

で，$p\nmid b_r$，$p\nmid c_0$ であるから $p\nmid a_r$（演習問題 52）となり仮定に反する．

例 14　$n>1$，a は 0 でも ±1 でもなく，平方因数をもたない整数ならば，

$$ f(x)=x^n+a $$

は $\boldsymbol{Q}$ で既約である．

実際，a の任意の素因数 p に対して，$p^2\nmid a$ であるから定理 2.26 が適用できる．この例はまた任意の n に対して $\boldsymbol{Q}$ で既約な n 次の多項式が存在すること

を示している．

例 15　pを素数とすれば，

$$f(x)=\frac{x^p-1}{x-1}=x^{p-1}+x^{p-2}+\cdots+x+1$$

は $\boldsymbol{Q}$ において既約である．この $f(x)$ を**円周等分多項式**とよんでいる．

$f(x)$ が $\boldsymbol{Q}$ で可約ならば，x を $x+1$ でおきかえた式

$$f(x+1)=(x+1)^{p-1}+(x+1)^{p-2}+\cdots+1$$
$$=\frac{(x+1)^p-1}{(x+1)-1}=\frac{(x+1)^p-1}{x}$$

も $\boldsymbol{Q}$ で可約である．二項定理によって

$$f(x+1)=x^{p-1}+px^{p-2}+\frac{p(p-1)}{2}x^{p-3}+\cdots+p.$$

ここで最初の項以外の係数はすべて p で割り切れるから定理 2.26 が適用できる．

$f(x)$ の根は $\cos\dfrac{2k\pi}{p}+i\sin\dfrac{2k\pi}{p}$ $(k=0,1,2,\cdots,p-1)$ であらわされ，すべて 1 の原始 p 乗根 (1.5 節例 7) である．

演習問題 2

1.　集合Sの部分集合の全体をRとする．Rの 2 元 A,B の和と積を

$$A+B=A\cup B-A\cap B,\quad AB=A\cap B$$

ときめれば，Rはこの演算に関して可換環をつくることを示せ．

2.　次の集合Rはかっこの中の演算に関して環をつくるか．

(1)　自然数の全体 (数の加法，乗法)．

(2)　有理数 $\dfrac{b}{a}$ で，$4\nmid a$ なるものの全体 (数の加法，乗法)．

(3)　実数を成分とする 2×2 行列で，対角成分が 0 のものの全体 (行列の加法，乗法)．

(4)　集合Sの部分集合の全体 (2 元 A,B の和と積を

$$A+B=A\cup B,\quad AB=A\cap B$$

ときめる)．

3.　2.1 節例 3 のRでは零元でない元は零因子か単元であることを示せ．

4.　2.1 節例 9 のRについて，次のことを示せ．

(1)　$I^2=J^2=K^2=-E.$

(2)　$IJ=-JI=K,\ JK=-KJ=I,\ KI=-IK=J.$

(3)　Rは環をつくる.

(4)　Rの元 $\alpha=aE+bI+cJ+dK$ に対して，$\alpha\neq 0$ ならば

$$\frac{1}{a^2+b^2+c^2+d^2}\cdot(aE-bI-cJ-dK)$$

は α の逆元である.

5.　a, b, c が環 R の元であるならば,

$$(-a)(-b)=ab, \quad a(b-c)=ab-ac$$

であることを示せ.

6.　$a_1, a_2, \cdots, a_m, b_1, b_2, \cdots, b_n$ が環 R の元ならば,

$$(a_1+a_2+\cdots+a_m)\cdot(b_1+b_2+\cdots+b_n)=\sum_{i=1}^{m}\sum_{j=1}^{n}a_ib_j$$

であることを示せ.

7.　環 R の 2 元 a, b と整数 m, n に対して

$$(ma)(nb)=(mn)ab$$

であることを示せ.

8.　環 R の単元の全体は乗法に関して群をつくることを示せ.

9.　ガウスの整数環 (2.1 節例10) の単元をすべてあげよ.

10.　環 R, R' の直積集合 $R\times R'=\{(a,b)\mid a\in R, b\in R'\}$ の 2 元 $(a,b), (a', b')$ の和と積を

$$(a,b)+(a',b')=(a+a', b+b')$$
$$(a,b)\cdot(a',b')=(aa', bb')$$

ときめて $R\times R'$ は環をつくることを示せ．この環を R, R' の**直積**とよぶ．また，$R\times R'$ は零因子をもつことを示せ.

11.　$R=\{a+b\sqrt{2}\mid a, b\in \boldsymbol{Z}\}$ は $\boldsymbol{R}$ の部分環ではあるが，部分体ではないことを示せ.

12.　$R=\{a+b\sqrt{2}\mid a, b\in \boldsymbol{Q}\}$ は $\boldsymbol{R}$ の部分体であることを示せ.

13.　素数 p に対して，$R=\left\{\dfrac{m}{n}\,\middle|\, m, n\in \boldsymbol{Z}\text{ で }n\text{ は }p\text{ と互いに素}\right\}$ は $\boldsymbol{Q}$ の部分環をつくることを示せ．また，Rの単元を求めよ.

14.　環 R の空でない部分集合 S に対して，S の各元と交換可能な R の元の全体は R の部分環をつくり，特に R が体のときは，部分体をつくることを示せ.

15.　R', R'' を環 R の部分環とするとき

$$R'\cup R''\text{ が部分環 }\Leftrightarrow R'\subseteqq R''\text{ または }R''\subseteqq R'$$

であることを示せ．2つの部分環の和集合が部分環にはならない例をあげよ．

16. A, B を環 R の空でない部分集合とする．A の元 a と B の元 b に対して $a+b$ なる形の R の元の全体を $A+B$，ab なる形の R の元を任意有限個加えたものの全体を $A\cdot B$ とかく．すなわち，

$$A+B=\{a+b \mid a\in A, b\in B\},$$

$$A\cdot B=\left\{\sum_{i=1}^{n} a_i b_i \mid a_i\in A, b_i\in B, n=1,2,\cdots\right\}.$$

A, B, C を空でない部分集合として，次のことを示せ．

(1) $(A\cdot B)\cdot C=A\cdot(B\cdot C)$，$A\cdot(B+C)\subseteqq A\cdot B+A\cdot C$.

(2) B, C が R の零元を含めば，(1)の第2式で等号が成り立つ．等号の成り立たない例もあげよ．

(3) A, B が加法群 R の部分群ならば，$A+B, A\cdot B$ も部分群である．

(4) A, B が R の左イデアルならば，$A+B, A\cdot B$ も左イデアルである．

(5) R が可換環で A, B が R の部分環ならば，$A\cdot B$ も R の部分環である．

17. 環 R の左イデアル $A_1, A_2, \cdots, A_n$ に対して，次のことを示せ．

(1) 和 $A_1+A_2+\cdots+A_n$ は $A_1, A_2, \cdots, A_n$ のすべてを含み，しかも，そのような R の左イデアルの中で最も小さい．

(2) 共通部分 $A_1\cap A_2\cap\cdots\cap A_n$ は，$A_1, A_2, \cdots, A_n$ のいずれにも含まれ，しかも，そのような R の左イデアルの中で最も大きい．

18. 演習問題1で $|S|=3$ として，環 R の部分環，イデアルをすべてあげよ．

19. 2.2節例5の証明をせよ．

20. $\boldsymbol{R}$ の上の2次の行列環 $(\boldsymbol{R})_2$ が単純環であることを示せ．

21. 環 R のイデアル A に対して

$$(A)_2=\left\{\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \middle| \ a_{ij}\in A,\ \ i,j=1,2\right\}$$

ときめて，次のことを示せ．

(1) $(A)_2$ は $(R)_2$ のイデアルである．

(2) $(R)_2$ の任意のイデアルは，適当な R のイデアル A に対して，$(A)_2$ の形であらわされる．

22. $\boldsymbol{R}$ の上の三角行列環を $R=\begin{pmatrix} \boldsymbol{R} & \boldsymbol{R} \\ 0 & \boldsymbol{R} \end{pmatrix}$ とかく．R の自明でないイデアルは

$$\begin{pmatrix} 0 & \boldsymbol{R} \\ 0 & 0 \end{pmatrix},\quad \begin{pmatrix} 0 & \boldsymbol{R} \\ 0 & \boldsymbol{R} \end{pmatrix},\quad \begin{pmatrix} \boldsymbol{R} & \boldsymbol{R} \\ 0 & 0 \end{pmatrix}$$

の 3 つにかぎられることを示せ.

23.　可換な単純環は体であることを示せ.

24.　A, B を環 R の左イデアルとし，$R=A+B$ であるとする．このとき自然数 m, n に対して

$$A^m+B=R, \quad A^m+B^n=R$$

であることを示せ．ここで $A^2=A\cdot A$, $A^3=A^2\cdot A, \cdots$ ときめる.

25.　環 R の元 a が**べき零**とは，ある自然数 n があって $a^n=0$ となることときめる．R が可換環のとき，べき零元全体の集合 N は R のイデアルであること，剰余環 R/N の零元でない元はべき零ではないことを示せ.

26.　$R=\{(a_{ij})\in(\boldsymbol{R})_n \mid a_{ij}=0\ (i>j)\}$, $S=\{(a_{ij})\in(\boldsymbol{R})_n \mid a_{ij}=0\ (i\geqq j)\}$, $T=\{(a_{ij})\in(\boldsymbol{R})_n \mid a_{ij}=0\ (i\neq j)\}$ とおく．次のことを示せ.

(1)　R, T は $(\boldsymbol{R})_n$ の部分環をなす.

(2)　S は R のイデアルである.

(3)　$R/S\cong T$ (環同型) である.

27.　R, S を環とする．任意の環準同型 $f\colon R\to S$ は，単射環準同型 f_1 と全射環準同型 f_2 によって $f=f_1f_2$ とかけることを示せ.

28.　$\boldsymbol{Z}$ から $\boldsymbol{Z}$ への環準同型は恒等写像しかないこと，$\boldsymbol{Q}$ から $\boldsymbol{Q}$ への環準同型も恒等写像しかないことを示せ.

29.　加法群 $\boldsymbol{Q}$ の自己準同型環は $\boldsymbol{Q}$ と環同型であること，自然数 m に対して，加法群 $\boldsymbol{Z}/(m)$ の自己準同型環もまた $\boldsymbol{Z}/(m)$ と環同型であることを示せ.

30.　p を素数とする．$\boldsymbol{Z}/(p)$ の元 $a+(p)$ の加法に関する逆元は $p-a+(p)$, $a+(p)\neq\bar{0}$ のときは $a^{p-2}+(p)$ が乗法に関する逆元であることを示せ.

31.　2.3 節例 12 の証明をせよ.

32.　R が環，A が R のイデアル，S が R の部分環とする．このとき，次のことを示せ.

(1)　$S+A$ は R の部分環.

(2)　A は $S+A$ のイデアルで，$S\cap A$ は S のイデアル.

(3)　$(S+A)/A\cong S/(S\cap A)$　　(環同型).

33.　R, S は環，$f\colon R\to S$ は環準同型とする．次のことを示せ.

(1)　R のイデアル A が $A\subseteqq \operatorname{Ker} f$ ならば，$g\pi=f$ をみたす環準同型 $g\colon R/A\to S$ がただ 1 つ存在する．ここで $\pi\colon R\to R/A$ は標準的準同型とする.

(2)　$\operatorname{Ker} g=(\operatorname{Ker} f)/A$.

34.　定理 2.8, 2.9 の証明をせよ.

35.　2.4 節の最後の L, M の環同型を示せ．

36.　整域 R の商体 M の元 $x_1, x_2, \cdots, x_n$ に対して，R の元 $a_1, a_2, \cdots, a_n$ と $b \neq 0$ とがあって

$$x_1=\alpha(a_1)\alpha(b)^{-1}, \cdots, x_n=\alpha(a_n)\alpha(b)^{-1}$$

とできることを示せ．

37.　2.5 節の $\bar{R}$ が可換環であることを示せ．

38.　補題 2.12 の証明をせよ．

39.　可換環 R の上のモニックな多項式は $R[x]$ の零因子とはなりえないことを示せ．

40.　可換環 R の上の 1 次式 $1+ax$ が $R[x]$ の単元である必要十分条件は，a が R のべき零元であることを示せ．

41.　体 K の上の多項式環 $K[x]$ では，x から生成されたイデアル

$$(x)=\{a_1x+a_2x^2+\cdots+a_nx^n \mid a_i \in K, n \geqq 1\}$$

は極大イデアルであることを示せ．

42.　可換環 R のイデアル A に対して

$$A[x]=\{a_0+a_1x+\cdots+a_nx^n \mid a_i \in A, n \geqq 0\}$$

は $R[x]$ のイデアルであって，

$$R[x]/A[x] \cong (R/A)[x] \qquad \text{(環同型)}$$

であることを示せ．

43.　(1)　$\boldsymbol{Z}/(2)$ と $\boldsymbol{Z}/(2)$ の直積を R とおく．R の上の多項式

$$f(x)=(1,0)x^2-(1,0)x$$

は R のすべての元を根にもつことを示せ．

(2)　$R=\boldsymbol{Z}/(4)$ で，$f(x)=\bar{2}x^2-\bar{2}x$ ではどうか．

44.　演習問題 13 の環 R は単項イデアル整域であることを示せ．

45.　ユークリッド整域 R は単項イデアル整域であることを示せ．

46.　α が $\alpha^2+\alpha+1=0$ をみたす 1 つの複素数ならば，$\boldsymbol{Z}[\alpha]=\{a+b\alpha \mid a, b \in \boldsymbol{Z}\}$ は単項イデアル整域であることを示せ．

47.　$a_1, a_2, \cdots, a_n$ を 0 でない整数とする．$a_1, a_2, \cdots, a_n$ の最小公倍数 l に対して，$\pm l$ は $a_1, a_2, \cdots, a_n$ の最小公倍元であり，また最小公倍元は $\pm l$ にかぎることを示せ．

48.　$a_1, a_2, \cdots, a_n$ を整域 R の 0 でない元とする．

$$a_1, a_2, \cdots, a_n \text{ が最小公倍元をもつ} \Leftrightarrow \bigcap_{i=1}^{n}(a_i) \text{ が単項イデアル}$$

であることを示せ．

49.　$\boldsymbol{Z}$ の素元は $\pm p$ (p は素数) であることを示せ.

50.　整域 R の素元が R の単元の約元となることはないことを示せ.

51.　p が整域 R の素元, u が R の単元ならば, pu は R の素元であることを示せ.

52.　p が一意分解整域 R の素元ならば, R の元 a, b に対して

$$p|ab \Rightarrow p|a \text{ または } p|b$$

であることを示せ.

53.　整域 R の単項イデアルの無限列 $(a_1)\subseteqq(a_2)\subseteqq\cdots$ に対して, 和集合 $\bigcup(a_i)$ がイデアルであることを示せ.

54.　R を一意分解整域, a, b は R の 0 でも単元でもない元とする. このとき

(1)　同じ素元 $p_1, p_2, \cdots, p_n$ を用いて

$$a=p_1{}^{e_1}p_2{}^{e_2}\cdots p_n{}^{e_n},\quad b=p_1{}^{f_1}p_2{}^{f_2}\cdots p_n{}^{f_n}\qquad (e_i\geqq 0, f_i\geqq 0)$$

とかけることを示せ.

(2)　a, b の最大公約元は

$$p_1{}^{m_1}p_2{}^{m_2}\cdots p_n{}^{m_n}\qquad (m_i=\min\{e_i, f_i\}\ \ (1\leqq i\leqq n))$$

で与えられることを示せ.

(3)　a, b の最小公倍元は何か.

55.　$\boldsymbol{C}[x]\ni f(x)=a_0+a_1x+\cdots+a_nx^n$ に対して, 多項式 $\bar{f}(x)$ を $\bar{f}(x)=\bar{a}_0+\bar{a}_1x+\cdots+\bar{a}_nx^n$ ときめる. ここで $\bar{a}_i$ は複素数 a_i の共役複素数をあらわす. このとき, 次のことを示せ.

(1)　写像 $\boldsymbol{C}[x]\to\boldsymbol{C}[x]$, $f(x)\to\bar{f}(x)$ は環同型である.

(2)　$\alpha\in\boldsymbol{C}$ に対して $\overline{f(\alpha)}=\bar{f}(\bar{\alpha})$ である.

(3)　$\alpha\in\boldsymbol{C}$ が $f(x)$ の根 $\Leftrightarrow$ $\bar{\alpha}$ が $\bar{f}(x)$ の根.

(4)　$f(x)\in\boldsymbol{R}[x]$ で, $\alpha\ (\in\boldsymbol{C})$ が $f(x)$ の根 $\Rightarrow$ $\bar{\alpha}$ も $f(x)$ の根である.

56.　可換環 R の $\{0\}$ でも R でもないイデアル A に対して, 写像 $\bar{\pi}$ を

$$\bar{\pi}\colon R[x]\to\bar{R}[x],\quad f(x)\to\bar{f}(x)$$

ときめる. ここで $\bar{R}=R/A$, $f(x)=a_0+a_1x+\cdots+a_nx^n$ に対して $\bar{f}(x)=\bar{a}_0+\bar{a}_1x+\cdots+\bar{a}_nx^n$, $\bar{a}_i=a_i+A\ (0\leqq i\leqq n)$ ときめる. 次のことを示せ.

(1)　$\bar{\pi}$ は全射環準同型で $\mathrm{Ker}\,\bar{\pi}=A[x]$.

(2)　$f(x)\in R[x]$ に対して $\bar{f}(x)$ が $\bar{R}[x]$ で既約ならば, $f(x)$ は $R[x]$ で既約である.

(3)　$f(x)=x^3-x^2+1$ は $\boldsymbol{Z}[x]$ で既約である.

57.　2.6 節例 13 の証明をせよ.

58. $f(x), g(x) \in \boldsymbol{Z}[x]$ で $g(x)$ は原始多項式とする．$\boldsymbol{Q}[x]$ で

$$f(x)=g(x)h(x)$$

とあらわされるならば，$h(x) \in \boldsymbol{Z}[x]$ であることを示せ．

59. $f(x)=x^5+x^4-2x^3+3$ を $\boldsymbol{Z}[x]$ で既約多項式の積にかけ．

60. $f(x)=x^4+1$ は $\boldsymbol{Q}[x]$ で既約であることを示せ．整数 a が 0 でないならば $g(x)=x^4-ax-1$ も $\boldsymbol{Q}[x]$ で既約であることを示せ．

3

加　　群

この章では，ベクトル空間の概念を拡張して環Rの上の加群を考え，加群のもつ性質が環Rを特徴づけることをみる．自由加群とよばれる加群を定義し，それを用いてアーベル群の基本定理を証明する．

3.1　加群と部分加群

Rを環，Mを加法群 (演算が加法のアーベル群を加法群とよんだ (1.1節)) とする．$R\times M$からMへの一意写像 $(a, x) \to ax$ があって，Rの任意の元 a, a' とMの任意の元 x, x' に対して

(1)　$a(x+x')=ax+ax'$,

(2)　$(a+a')x=ax+a'x$,

(3)　$(aa')x=a(a'x)$,

(4)　$1\cdot x=x$

の4つの条件が成り立つとき，MをRの上の**左加群**，または**R-左加群**とよび，${}_RM$ であらわす．ここで1はRの単位元をあらわす．

R-右加群Nも同じように定義できる．これは N_R であらわす．

Rが可換環のときは，R-右加群はR-左加群ともみられる．実際，R-右加群Nの任意の元 y とRの任意の元 b に対して，Nの元 yb がきまる．いま $by=yb$ とおいて，$R\times N$からNへの写像 $(b, y) \to by$ をきめる．Rの任意の元 b, b' に対して $(bb')y=y(bb')$ であり，

$$b(b'y)=(b'y)b=(yb')b=y(b'b)=y(bb')$$

であるから，$(bb')y=b(b'y)$ が成り立つ．他の条件が成り立つことは明らか

で，NはR-左加群となる．

同じようにRが可換環ならば，R-左加群はR-右加群でもあり，左加群，右加群の区別はいらない．

例 1 環Rが$\boldsymbol{R}$のとき，上にのべたR-左加群の定義は$\boldsymbol{R}$の上のベクトル空間の定義と全く同じである．一般に，Rが斜体であるとき，R-左加群，R-右加群をそれぞれRの上の**左ベクトル空間**，**右ベクトル空間**とよんでいる．

例 2 アーベル群Gは$\boldsymbol{Z}$の上の(左)加群である．Gの演算を加法でかき，写像$\boldsymbol{Z}\times G\to G$を$(n, a)\to na$ときめるとよい．ここで$na$は

$$na=\begin{cases} a \text{ の } n \text{ 個の和} & (n>0 \text{ のとき}), \\ 0 & (n=0 \text{ のとき}), \\ -a \text{ の } |n| \text{ 個の和} & (n<0 \text{ のとき}) \end{cases}$$

をあらわす(1.1節参照)．

このように環Rの上の左加群の概念は，ベクトル空間の概念の拡張であり，またアーベル群の概念の拡張にもなっている．

例 3 環R自身R-左加群であり，またR-右加群でもある．写像$R\times R\to R$を$(a, b)\to ab$ときめたらよい．ここでabはRの元a, bのRにおける積をあらわす．

例 4 n個の実数の組$(a_1, a_2, \cdots, a_n)$の全体を$\boldsymbol{R}^n$とかく．$\boldsymbol{R}^n$が$\boldsymbol{R}$の上のベクトル空間をつくることはよく知られている．$\boldsymbol{R}^n$の加法を

$$(a_1, a_2, \cdots, a_n)+(b_1, b_2, \cdots, b_n)=(a_1+b_1, a_2+b_2, \cdots, a_n+b_n)$$

ときめ，スカラー積を実数aに対して

$$a\cdot(a_1, a_2, \cdots, a_n)=(aa_1, aa_2, \cdots, aa_n)$$

ときめた．

全く同じように，Rを環とし，n個のRの直積集合$R\times R\times\cdots\times R$を$R^n$とかく．

$$R^n=\{(a_1, a_2, \cdots, a_n)\mid a_1, a_2, \cdots, a_n\in R\}.$$

R^nの加法は上と同じように

$$(a_1, a_2, \cdots, a_n)+(b_1, b_2, \cdots, b_n)=(a_1+b_1, a_2+b_2, \cdots, a_n+b_n)$$

ときめ，写像$R\times R^n\to R^n$を

$$(a, (a_1, a_2, \cdots, a_n))\to(aa_1, aa_2, \cdots, aa_n)$$

ときめてR^nはR-左加群となる．R^nの零元は$(0, 0, \cdots, 0)$である．また，R^nをR-右加群にすることもできる．

特に，$n=1$のとき，R^nは例3のRと一致する．

例 5　加法群Mの自己準同型環End(M) (2.1節例3)をRとおく．このとき写像$R\times M\to M$を$(f,x)\to f(x)$ときめて，MをR-左加群にすることができる．

fが準同型であるから条件(1)が成り立つ．条件(2),(3)はRの加法，乗法のきめ方による．(4)はMの恒等写像がRの単位元であることによる．

これからはR-左加群を主にあつかうので，これを単にR-加群とよぶことにする．次の補題は補題2.1と同じようにして証明できる．

補題 3.1　Rを環，MをR-加群とし，R, Mの零元をそれぞれ$0_R, 0_M$とかけば，

(1)　任意の$x\in M$に対して$0_R x=0_M$.

(2)　任意の$a\in R$に対して$a0_M=0_M$.

(3)　任意の$a\in R, x\in M$に対して

$$(-a)x=-ax=a(-x).$$

この補題から零加法群はいつもR-加群である．これを**零加群**とよんでいる．

これからは特に必要がないかぎり，Rの零元，Mの零元を単に0とかき，$0_R, 0_M$と区別してかくことはしない．前後の関係から0がRの零元か，Mの零元かは判断できる．

MをR-加群とする．加法群Mの部分群M'が

$$x\in M', a\in R \Rightarrow ax\in M'$$

をみたすとき，M'をMの**部分加群**とよぶ．このとき，M'自身1つのR-加群となる．M自身も，Mの零元のみからなるMの部分群もMの部分加群である．この2つをMの**自明な部分加群**とよぶ．次の補題は定理1.5から分かる．

補題 3.2　MをR-加群，M'をMの部分集合とする．

M'がMの部分加群 $\Leftrightarrow$ (1)　$x, y\in M' \Rightarrow x-y\in M'$,

(2)　$0\in M'$,

(3)　$x\in M'$,　$a\in R \Rightarrow ax\in M'$.

例1の$\boldsymbol{R}$の上のベクトル空間では，部分空間が部分加群にほかならない．

例2では，アーベル群Gのすべての部分群が部分加群である．

例3では，RをR-左加群とみれば，Rの部分加群はRの左イデアルを意味し，RをR-右加群とみれば，Rの部分加群はRの右イデアルを意味する．

R-加群Mの元xに対して，Rxを

$$Rx=\{ax\in M \mid a\in R\}$$

ときめる．補題3.2を用いて Rx がMの部分加群であることが分かる．Rx は $1\cdot x=x$ を含む．x を含むMの部分加群はすべて Rx を含むから，Rx は x を含むMの部分加群の中で最小である．この Rx を x から生成されたMの**巡回部分加群**とよぶ．

例1では，1次元の部分空間が巡回部分加群である．

例2では，1.2節例9の x から生成されたGの巡回部分群

$$(x)=\{mx \mid m\in \boldsymbol{Z}\}$$

が x から生成されたGの巡回部分加群 $\boldsymbol{Z}x$ にほかならない．

例3では，R-左加群Rの巡回部分加群はRの単項左イデアルのことであり，R-右加群Rの巡回部分加群はRの単項右イデアルのことである．

この章では，Rの元 a から生成された単項左イデアルを (a) とはかかずに，Rの部分加群という意味を強調して，Ra とかく(2.2節例2)．しかし，$R=\boldsymbol{Z}$ では，$\boldsymbol{Z}a$ とはかかず従来通り (a) とかく．これは a の倍数の全体であった．

部分加群が自明のものしかない R-加群を**単純加群**という．Mが R-加群で $M\neq\{0\}$ のときは

$$M\text{が単純加群} \Leftrightarrow x\in M, x\neq 0 \text{ ならば } M=Rx$$

が成り立つ．

実際，$\Rightarrow$ は明らかで，$\Leftarrow$ を示すために M' を $\{0\}$ でないMの部分加群とする．0でない元 x が M' にあり，仮定から $M=Rx\subseteqq M'\subseteqq M$ で，$M'=M$ となりMは単純加群である．

例 6　アーベル群Gを，例2のように $\boldsymbol{Z}$-加群とみたとき，$G\neq\{0\}$ ならば，

$$G\text{が単純加群} \Leftrightarrow G\text{ の位数は素数}$$

である(1.5節例4)．

例 7　定理2.4から環Rに対して

$$R\text{が斜体} \Leftrightarrow {}_RR\text{ が単純加群} \Leftrightarrow R_R\text{ が単純加群}$$

が成り立つ．

R-加群Mの部分加群 $M_1, M_2, \cdots, M_n$ に対して

$$M_1+M_2+\cdots+M_n=\{x_1+x_2+\cdots+x_n \mid x_i\in M_i, 1\leqq i\leqq n\}$$

とおき，$M_1, M_2, \cdots, M_n$ の**和**とよぶ．これはMの部分加群をつくる．

実際，$M_1+M_2+\cdots+M_n$ の2元 $x=x_1+x_2+\cdots+x_n$,　$x'=x_1'+x_2'+\cdots$

$+x_n'$ に対して $x-x'=(x_1-x_1')+(x_2-x_2')+\cdots+(x_n-x_n')$ は $M_1+M_2+\cdots+M_n$ に属する．Mの零元0は各 M_i に属し，$0+0+\cdots+0=0$ から $M_1+M_2+\cdots+M_n$ はMの零元を含む．$M_1+M_2+\cdots+M_n$ の元 $x=x_1+x_2+\cdots+x_n$ とRの元 a に対して $ax=ax_1+ax_2+\cdots+ax_n$ は $ax_i\in M_i$ であるから，また $M_1+M_2+\cdots+M_n$ に属する．補題3.2から $M_1+M_2+\cdots+M_n$ はMの部分加群である．

明らかに，$M_1+M_2+\cdots+M_n$ は $M_1, M_2, \cdots, M_n$ のすべてを含み，かつ，そのようなMの部分加群の中で最小である．

Mを R-加群とする．Mの空でない部分集合Sに対して，Sを含むMの部分加群全部の共通部分は補題3.2からMの部分加群をつくる．この部分加群はSを含むMの部分加群の中で最小であり，これをSから**生成**されたMの部分加群とよぶ(1.2節例7)．

Rの元 a とSの元 x に対して ax なる形のMの元の有限和の全体を $R\cdot S$ とかく．

$$R\cdot S=\left\{\sum_{i=1}^{n} a_ix_i \,\middle|\, a_i\in R,\ \ x_i\in S,\ \ n=1,2,\cdots\right\}.$$

$R\cdot S$ はSから生成されたMの部分加群である．

実際，補題3.2から $R\cdot S$ はMの部分加群であり，Sの任意の元 x に対して $x=1\cdot x\in R\cdot S$ であるからSを含む．Sを含むMの任意の部分加群は，Rの元 a とSの元 x とに対して，ax なる形のMの元を含み，したがって，そのようなものの有限個の和を含むから $R\cdot S$ を含む．すなわち，$R\cdot S$ はSを含むMの部分加群の中で最小である．

特に，$S=\{x\}$ のとき $R\cdot S$ は巡回部分加群 Rx に等しく，$S=\{x_1, x_2, \cdots, x_n\}$ のときは $R\cdot S$ は巡回部分加群の和 $Rx_1+Rx_2+\cdots+Rx_n$ に等しい．また，Mの部分加群 $M_1, M_2, \cdots, M_n$ に対して $S=M_1\cup M_2\cup\cdots\cup M_n$ とおけば，$R\cdot S=M_1+M_2+\cdots+M_n$ が成り立つ．これらの証明は演習問題とする．

R-加群MがMのある巡回部分加群 $Rx_1, Rx_2, \cdots, Rx_n$ の和に等しいとき，すなわち，Mの元 $x_1, x_2, \cdots, x_n$ があって

$$M=Rx_1+Rx_2+\cdots+Rx_n$$

であるとき，Mを有限生成 R-加群または単に**有限生成加群**，$x_1, x_2, \cdots, x_n$ をMの**生成元**とよぶ．

特に，$n=1$ であるとき，すなわち，Mの元 x があって

$$M=Rx$$

であるとき，Mを巡回 R-加群または単に**巡回加群**とよぶ．

例1の $\boldsymbol{R}$ の上のベクトル空間Mでは，$M\neq\{0\}$ ならばMが有限生成加群とはMが有限次元であることを，Mが巡回加群とはMの次元が1であることを意味する．このことはMの生成元の中から基底がとれることに注意したらよい．

例3でRを R-加群とみれば，Rの単位元1に対して $R=R1$ であるから，R は巡回加群である．a がRの単元ならば $R=Ra$ も成り立つから，Rは単元から生成された巡回加群ということもできる．

例 8 例4の R^n で，$1\leqq i\leqq n$ なる i に対して

$$R_i=\{(0,\cdots,0,\overset{i}{\breve{a}},0,\cdots,0)\mid a\in R\}$$

は R^n の部分加群であり，

$$(a_1,a_2,\cdots,a_n)=(a_1,0,\cdots,0)+(0,a_2,0,\cdots,0)+\cdots+(0,\cdots,0,a_n)$$

であるから，R^n は部分加群 $R_1,R_2,\cdots,R_n$ の和に等しい．

$$R^n=R_1+R_2+\cdots+R_n.$$

$1\leqq i\leqq n$ なる i に対して，R^n の元 e_i を

$$e_i=(0,\cdots,0,\overset{i}{\breve{1}},0,\cdots,0)$$

ときめれば，R_i は巡回部分加群 Re_i に一致し，

$$R^n=Re_1+Re_2+\cdots+Re_n$$

は R^n が $e_1,e_2,\cdots,e_n$ を生成元とする有限生成加群であることを示す．

例 9 2つの整数 a,b に対して，1.2節例4から $S=\{a,b\}$ から生成された加法群 $\boldsymbol{Z}$ の部分群（1.2節例9）はSから生成された部分加群でもあり，これは $\boldsymbol{Z}$ の巡回部分加群 $\boldsymbol{Z}a,\boldsymbol{Z}b$ の和に等しい．

もし a,b が互いに素ならば，$xa+yb=1$ をみたす整数 x,y が存在するから，

$$\boldsymbol{Z}=\boldsymbol{Z}a+\boldsymbol{Z}b$$

が成り立つ．

$\boldsymbol{Z}$ は1から生成された巡回加群であり，また，互いに素な2つの整数を生成元とする有限生成加群でもある．このことは，一般には，有限生成加群の生成元が一通りではないことを，その個数も一定とはかぎらないことを示している．

R-加群Mの部分加群 M_0 がMの**極大部分加群**であるとは

(1) $M_0\neq M$,

(2)　M_0 を含む M の部分加群は M_0 か M にかぎられる

ときめる．

次の補題は有限生成 R-加群はいつも極大部分加群をもつことを示している．

補題 3.3　M が有限生成 R-加群，M' が M の部分加群で $M \neq M'$ ならば，M' を含む M の極大部分加群が存在する．

特に，有限生成 R-加群は極大部分加群をもつ．したがって，R 自身極大左(右)イデアル，また極大イデアルをもつ．

証明　M の部分加群で M' を含み M と異なるものの全体を $\mathcal{A}$ とする．$\mathcal{A}$ は包含関係に関して順序集合をつくる．$\mathcal{A}$ は M' を含むから空ではない．

$\mathcal{A}$ が帰納的であることを示す．$\{M_\lambda \mid \lambda \in \Lambda\}$ を $\mathcal{A}$ の任意の全順序部分集合とすると $\cup_\Lambda M_\lambda$ は M' を含む M の部分加群である．もし $\cup_\Lambda M_\lambda = M$ ならば，M の生成元全部を含むある M_λ が存在し，$M = M_\lambda$ となって矛盾である．$\cup_\Lambda M_\lambda \neq M$ で，したがって，$\cup_\Lambda M_\lambda \in \mathcal{A}$.

ツォルンの補題から $\mathcal{A}$ は極大元 M_0 をもつ．M_0 が M' を含む M の極大部分加群であることを示す．$M_0 \in \mathcal{A}$ から $M' \subseteqq M_0 \subsetneqq M$ である．M'' が M の部分加群で $M_0 \subseteqq M'' \subsetneqq M$ ならば，$M'' \in \mathcal{A}$ であり，M_0 の極大性から $M'' = M_0$.

後半の証明は $M' = 0$ とおけばよい．

M を R-加群，M' を M の部分加群とする．M' は加法群 M の正規部分群であるから，剰余群 M/M' がつくれる．このとき R の元 a，M/M' の元 $x+M'$ に対して

$$a \cdot (x+M') = ax + M'$$

ときめると，写像

$$R \times M/M' \to M/M', \quad (a, x+M') \to a \cdot (x+M')$$

は一意写像であり，この節のはじめにあげた4つの条件をみたす．こうして M/M' を R-加群とすることができる．この R-加群を M の M' による**剰余加群**とよぶ．

剰余加群 M/M' の部分加群がどんなものであるかを調べてみよう．

M/M' の部分加群は，まず剰余群 M/M' の部分群であるから

$$M_1/M', \quad M_1 \text{ は } M \text{ の部分群で } M' \subseteqq M_1$$

の形をしている (定理 1.20)．その上，任意の R の元 a と M_1 の元 x_1 に対して

$$ax_1 + M' = a \cdot (x_1 + M') \in M_1/M'$$

でなければならない．ある $x_1' \in M_1$ があって $ax_1 + M' = x_1' + M'$．したがって

$ax_1-x_1'\in M'$. $ax_1-x_1'=x_2$ をみたす M' の元 x_2 がある.

$$ax_1=x_1'+x_2\in M_1+M'\subseteqq M_1.$$

このことは M_1 がMの部分加群であることを示している.

逆に, Mの部分加群 M_1 が M' を含めば M_1/M' が M/M' の部分加群をつくることは明らかで, したがって, 剰余加群 M/M' の部分加群とは

$$M_1/M',\ M_1 \text{ は} M \text{の部分加群で } M'\subseteqq M_1$$

によってつくされる.

例 10 環Rを R-加群とみれば, Rの部分加群はRの左イデアルであった. Aを左イデアルとして剰余加群 R/A を考える. この剰余加群の部分加群は

$$A_1/A,\ A_1 \text{ は} A \text{を含む} R \text{の左イデアル}$$

でつくされる.

例えば, Aが極大左イデアルならば, A_1 はRかAにかぎられるから R/Aは単純加群である. Rが単項イデアル整域で, p がRの素元のとき, 剰余加群 R/Rp は単純加群である(補題 2.18).

例 11 Rを単項イデアル整域, pをRの素元, eを自然数として剰余加群 R/Rp^e を考え, その部分加群を求めてみる.

R/Rp^e の部分加群は

$$Ra/Rp^e,\ Ra \text{ は } Rp^e \text{ を含む} R \text{のイデアル}$$

の形をしている. $p^e\in Ra$ からあるRの元 b があって $p^e=ab$. a が単元でないならば, $a\neq 0$ から素元分解の一意性により

$$a=up^f \qquad (u \text{ は} R \text{の単元},\ 0\leqq f\leqq e).$$

したがって, $Ra=Rp^f$ で, R/Rp^e の自明でない部分加群は

$$Rp^{e-1}/Rp^e, Rp^{e-2}/Rp^e, \cdots, Rp/Rp^e$$

でつくされる. R/Rp^e の部分加群は

$$\{\bar{0}\}\subsetneqq Rp^{e-1}/Rp^e\subsetneqq Rp^{e-2}/Rp^e\subsetneqq\cdots\subsetneqq Rp/Rp^e\subsetneqq R/Rp^e$$

と一列に並ぶ.

例 12 有限生成 R-加群の剰余加群はまた有限生成加群であるが, 部分加群はかならずしもそうではない.

$M=Rx_1+Rx_2+\cdots+Rx_n$ が有限生成加群ならば, Mの剰余加群 M/M' は x_1+M', x_2+M', $\cdots$, x_n+M' を生成元とする有限生成加群である.

例えば, 2.1節例3にのべたように, $\boldsymbol{R}$ から $\boldsymbol{R}$ への写像の全体 R は可換環をつくる. このRを R-加群とみれば巡回加群, したがって, 有限生成加群である. Rの部分加群 R' を次のようにきめる.

$$R'=\{f\in R \mid ある\ n\geqq 0\ があって\ |x|>n\ ならば\ f(x)=0\}.$$

R' が有限生成加群で，$f_1, f_2, \cdots, f_k$ がその生成元と仮定する．各 f_i に対してきまる n の中で最大なものを m とかけば，R' の任意の元 f は $f=\sum_{i=1}^{k} a_i f_i$ $(a_i\in R)$ とかけるから

$$|x|>m \quad ならば \quad f(x)=0$$

となる．しかし，例えば，

$$f(x)=\begin{cases}1 & (-m-1\leqq x\leqq m+1),\\ 0 & (|x|>m+1)\end{cases}$$

と f をきめると，この f は上の関係をみたさない．

3.2　加群の準同型

M, N を R-加群とする．M から N への写像 $f: M\to N$ が M の任意の元 x, x' と R の任意の元 a とに対して

$$f(x+x')=f(x)+f(x'),$$
$$f(ax)=a\cdot f(x)$$

をみたすとき，f を M から N への R-**準同型写像**または単に R-**準同型**とよぶ．単射 R-準同型，全射 R-準同型などは群の場合と同様であり，全単射 R-準同型 f を R-**同型**とよび，このとき $M\cong^{f} N$ とあらわすこと等も群の場合と同様である．

f が R-準同型ならば，$f(x-x')=f(x+(-x'))=f(x)+f(-x')=f(x)-f(x')$ であることを注意しておこう．

M のすべての元を N の零元にうつす写像 $0: M\to N$ は R-準同型であり，これを**零写像**とよぶ．M の元 x をそのまま x にうつす写像 $1_M: M\to M$ は R-同型で，これを M の**恒等写像**とよぶ．

R-準同型 $f: M\to N$ に対して，f の像

$$f(M)=\{f(x)\mid x\in M\}$$

は N の部分加群であり，f の核

$$\mathrm{Ker}\, f=\{x\in M\mid f(x)=0\}$$

は M の部分加群である．もっと一般に，M, N の部分加群 M', N' に対して，f による M' の像 $f(M')$，f による N' の原像 $f^{-1}(N')$ はそれぞれ N, M の部分加群である．

群の場合と同様に

$$f\text{が全射} \Leftrightarrow f(M)=N, \quad f\text{が単射} \Leftrightarrow \mathrm{Ker}\, f=\{0\}$$

が成り立つ．

例 1 $\boldsymbol{R}$ の上のベクトル空間 M, N を $\boldsymbol{R}$-加群とみたとき，$\boldsymbol{R}$-準同型 $f\colon M \to N$ とは $\boldsymbol{R}$-線型写像を意味する．

アーベル群 G, H を $\boldsymbol{Z}$-加群とみたとき，加法群 G から加法群 H への準同型 $f\colon G \to H$ はすべて $\boldsymbol{Z}$-準同型となる．それは $\boldsymbol{Z}$-準同型の第一の条件 $f(x+x')=f(x)+f(x')$ が自然に第二の条件 $f(ax)=a\cdot f(x)$ をみちびくからである．

例 2 M を R-加群，M' を M の部分加群とする．M' の元 x を M の元とみて写像 ν を

$$\nu\colon M' \to M, \quad x \to x$$

ときめれば，ν は一意写像であり，単射 R-準同型で ν の像 $\nu(M')$ は M' に等しい．ν を M' から M への**包含写像**とよぶ．

M の M' による剰余加群 M/M' をつくり，写像 π を

$$\pi\colon M \to M/M', \quad x \to x+M'$$

ときめれば，π は一意写像であり，全射 R-準同型で $\mathrm{Ker}\, \pi$ は M' に等しい．π を M から M/M' への**標準的**または**自然な** R-準同型とよぶ．

例 3 M, N を R-加群，$f\colon M \to N$ を R-準同型とする．M の部分加群 M' に対して，包含写像 $\nu\colon M' \to M$ と f とを合成した写像

$$f\nu\colon M' \to N$$

も R-準同型である．この写像を $f|_{M'}$ とかき，f の M' への**制限写像**とよぶ．この写像の核は

$$\mathrm{Ker}\, f|_{M'} = \mathrm{Ker}\, f \cap M'$$

で与えられる．

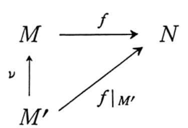


図 3.1

剰余加群 M/M' から剰余加群 $N/f(M')$ への写像 $\bar{f}$ を

$$\bar{f}\colon M/M' \to N/f(M'), \quad x+M' \to f(x)+f(M')$$

ときめれば，$\bar{f}$ も一意写像であり R-準同型で

$$\pi_N f = \bar{f}\pi_M$$

が成り立つ．この $\bar{f}$ を f から**誘導**された R-準同型とよぶ．ここで $\pi_M\colon M\to M/M'$, $\pi_N\colon N\to N/f(M')$ は共に標準的な R-準同型をあらわす．

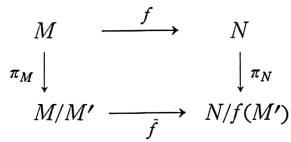


図 3.2

図 3.1 は 3 つの R-加群と 3 つの R-準同型からなる図型で，M' から N へ向かう 2 つの R-準同型 $f\nu$ と $f|_{M'}$ とがあって一致している．このようなときこの図型は**可換図型**であるという．図 3.2 では $\pi_N f=\bar{f}\pi_M$ が図型の可換性を示している．図型が可換であることをあらわすのに $\circlearrowright$ という記号を用いる．例えば，図 3.1 では図 3.3 のようにかく．

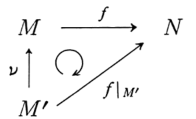


図 3.3

例 4 M, N を R-加群，$f\colon M\to N$ を R-準同型とする．このとき $\mathrm{Ker}\, f$ は M の部分加群で，f から誘導された写像

$$\bar{f}\colon M/\mathrm{Ker}\, f\to N,\quad x+\mathrm{Ker}\, f\to f(x)$$

は単射 R-準同型で（$f(\mathrm{Ker}\, f)=\{0\}$ に注意），したがって，

$$M/\mathrm{Ker}\, f\cong^{\bar{f}} f(M)$$

が成り立つ．これを R-加群の**準同型定理**とよぶ．

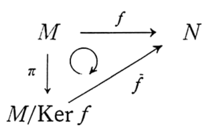


図 3.4

例 5 $M=Rx$ を x から生成された巡回加群とする．写像

$$f\colon R\to Rx,\quad a\to ax$$

は一意写像であり，全射 R-準同型で，例 4 から

$$R/\mathrm{Ker}\, f\cong^{\bar{f}} Rx$$

が成り立つ．Ker f は

$$\{a \in R \mid ax=0\}$$

で与えられる R の左イデアルである．これを x の**左零化イデアル**とよび，$\mathrm{Ann}_R\, x$ であらわす．

逆に，R の左イデアル A に対して，剰余加群 R/A は $1+A$ を生成元とする巡回加群 $R\cdot(1+A)$ で，したがって，巡回加群とは適当な R の左イデアル A に対して R/A と R-同型であり，かつ，このようなものにかぎられる．

$M=Rx$ を巡回加群とする．x の左零化イデアルに対して

$$\bigcap_{m\in M} \mathrm{Ann}_R\, m = \{a\in R \mid \text{すべての } m\in M \text{ に対して } am=0\}$$

を M の左零化イデアルといい，$\mathrm{Ann}_R\, M$ であらわす．R が可換ならば

$$\mathrm{Ann}_R\, M = \mathrm{Ann}_R\, x$$

が成り立つ．

R が可換環で，M が巡回加群，$a\in R$ ならば

$$M\cong R/Ra \iff \mathrm{Ann}_R\, M = Ra.$$

実際，R/Ra は $1+Ra$ の生成元とする巡回加群であるから，$b\in R$ に対して

$$bM=\{0\} \iff b\cdot R/Ra=\{0\} \iff b\cdot(1+Ra)=0 \iff b\in Ra$$

が成り立つ．

例 6　$M=Rx_1+Rx_2+\cdots+Rx_n$ を有限生成加群とすると

$$\alpha\colon R^n \to M, \quad (a_1, a_2, \cdots, a_n) \to \textstyle\sum_{i=1}^n a_i x_i$$

は一意写像で全射 R-準同型である．ここで R^n は 3.1 節例 4 の R-加群である．

このことの逆も成り立ち，一般に，R-加群 M に対して

$$M \text{ が有限生成} \iff \text{ある } n \text{ と全射 } R\text{-準同型 } R^n \to M \text{ が存在する．}$$

逆の証明をする．全射 R-準同型 $R^n\to M$ を f とおくと，図 3.5 の図型は可換

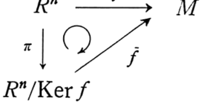


図 3.5

図型である．R^n は有限生成 (3.1 節例 8)，その剰余加群 $R^n/\mathrm{Ker}\, f$ も有限生成 (3.1 節例 12) である．したがって，同型な M も有限生成である．

例 7　3.1 節例 11 で，単項イデアル整域 R の素元 p に対して，剰余加群 R/Rp^e の部分加群が

$$Rp^f/Rp^e \qquad (0 \leqq f \leqq e)$$

でつくされることを示したが，

$$Rp^f/Rp^e \cong R/Rp^{e-f}$$

が成り立ち，R/Rp^e の部分加群はすべて巡回加群であることが分かる．

これには写像 h: $R/Rp^{e-f} \to Rp^f/Rp^e$ を

$$a+Rp^{e-f} \to ap^f+Rp^e$$

ときめると，h は一意写像で，全単射 R-準同型であることに注意したらよい．

M を R-加群とする．M はまず加法群であるから M の自己準同型全部をあつめて環 $\mathrm{End}(M)$ ができる．M は R-加群であるから M から M への R-準同型(これを M の R-**自己準同型**とよぶ)が考えられる．この全体を $\mathrm{End}({}_RM)$ とかく．明らかに

$$\mathrm{End}({}_RM) \subseteqq \mathrm{End}(M)$$

であるが，実は $\mathrm{End}({}_RM)$ は $\mathrm{End}(M)$ の部分環である．

補題 2.2 を用いてこのことを確かめてみよう．まず，M の恒等写像 1_M は M の R-自己準同型であるから，$\mathrm{End}({}_RM)$ は空ではなく，また $\mathrm{End}(M)$ の単位元を含んでいる．$f, g \in \mathrm{End}({}_RM)$ ならば，$a \in R, x \in M$ に対して

$$f(ax)-g(ax)=a\cdot f(x)-a\cdot g(x)=a\cdot(f(x)-g(x)),$$
$$f(g(ax))=f(a\cdot g(x))=a\cdot f(g(x))$$

となるから $f-g, fg \in \mathrm{End}({}_RM)$ で，$\mathrm{End}({}_RM)$ は $\mathrm{End}(M)$ の部分環をつくる．

R-加群 M, N に対して，M から N への R-準同型の全体を

$$\mathrm{Hom}_R(M, N)$$

とかく．$\mathrm{Hom}_R(M, N)$ は自然な方法で加法群をつくる．この証明は演習問題とする．上にのべたことは，$M=N$ ならば，$\mathrm{Hom}_R(M, M)=\mathrm{End}({}_RM)$ が環でもあることを示している．この環を M の R-**自己準同型環**とよんでいる．

3.3　加群の直和

M を R-加群，$M_1, M_2, \cdots, M_n$ を M の部分加群とする．このとき，M が $M_1, M_2, \cdots, M_n$ の**内部直和**であるとは

(1)　$M=M_1+M_2+\cdots+M_n$,

(2) $i=1,2,\cdots,n$ に対して $M_i\cap\sum_{j\neq i}M_j=\{0\}$

であるときめる．

$M_1, M_2, \cdots, M_n$ の内部直和を

$$M=M_1\oplus M_2\oplus\cdots\oplus M_n,\quad \text{または}\ M=\oplus_{i=1}^{n}M_i$$

であらわす．これをMの**直和分解**とも，Mは $M_1, M_2, \cdots, M_n$ の**直和に分解される**ともいう．$M_1, M_2, \cdots, M_n$ のそれぞれをMの**直和因子**とよぶ．

Mの直和分解はMの元によっても特徴づけることができる．

定理 3.4 R-加群Mの部分加群 $M_1, M_2, \cdots, M_n$ に対して

Mが $M_1, M_2, \cdots, M_n$ の内部直和

$\Leftrightarrow$ Mの任意の元xが

$$x=x_1+x_2+\cdots+x_n \qquad (x_i\in M_i,\ 1\leqq i\leqq n)$$

の形に一意的にあらわされる．

証明 Mが内部直和とする．Mは $M_1, M_2, \cdots, M_n$ の和であるから，Mの元xは $x=x_1+x_2+\cdots+x_n$ $(x_i\in M_i)$ とかける．もし $x=x_1+x_2+\cdots+x_n=y_1+y_2+\cdots+y_n$ $(x_i, y_i\in M_i)$ と二通りにあらわされるならば，各 i に対して $x_i-y_i=-\sum_{j\neq i}(x_j-y_j)$ となる．この式の左辺は M_i に属し，右辺は $\sum_{j\neq i}M_j$ に属するから，$x_i-y_i=0, x_i=y_i$ となってあらわし方は一意的である．

逆に，Mの元xが $x=x_1+x_2+\cdots+x_n$ $(x_i\in M_i)$ の形にかけることは $M=M_1+M_2+\cdots+M_n$ を意味する．各 i に対して，$M_i\cap\sum_{j\neq i}M_j$ の任意の元は $x_i=\sum_{j\neq i}x_j$ $(x_i\in M_i, 1\leqq i\leqq n)$ とあらわされる．この両辺を

$$0+\cdots+0+\overset{i}{\breve{x_i}}+0+\cdots+0=x_1+x_2+\cdots+x_{i-1}+\overset{i}{\breve{0}}+x_{i+1}+\cdots+x_n$$

とかきなおして一意性の条件を用いると $x_i=0$ をうる．したがって，$M_i\cap\sum_{j\neq i}M_j=\{0\}$ である．

例 1 Mを$\boldsymbol{R}$の上のベクトル空間，$x_1, x_2, \cdots, x_n$ をMの基底とする．$x_1, x_2, \cdots, x_n$ はMの生成元であり，かつ，1次独立である．生成元であることはMの任意の元xが

$$x=a_1x_1+a_2x_2+\cdots+a_nx_n \qquad (a_i\in\boldsymbol{R},\ 1\leqq i\leqq n)$$

とあらわされることを意味する．その上，もしxが $x=a_1x_1+a_2x_2+\cdots+a_nx_n=b_1x_1+b_2x_2+\cdots+b_nx_n$ $(a_i, b_i\in\boldsymbol{R}, 1\leqq i\leqq n)$ と二通りにあらわされるならば，

$$(a_1-b_1)x_1+(a_2-b_2)x_2+\cdots+(a_n-b_n)x_n=0.$$

$x_1, x_2, \cdots, x_n$ は1次独立であるから

$$a_1-b_1=a_2-b_2=\cdots=a_n-b_n=0,$$

$$a_1=b_1, a_2=b_2, \cdots, a_n=b_n$$

となり，あらわし方は一意的である．したがって，Mは巡回部分加群 $\boldsymbol{R}x_1, \boldsymbol{R}x_2, \cdots, \boldsymbol{R}x_n$ の内部直和である．

例 2　Mを$\boldsymbol{R}$の上の有限次ベクトル空間，M'をMの部分空間とし，M'の基底を $x_1, x_2, \cdots, x_m$ とする．よく知られたように，$x_1, x_2, \cdots, x_m$ に適当なMの元 $x_{m+1}, \cdots, x_n$ をつけ加えて

$$x_1, x_2, \cdots, x_m, x_{m+1}, \cdots, x_n$$

がMの基底であるようにできる．例 1 から

$$\begin{aligned} M&=\boldsymbol{R}x_1\oplus\boldsymbol{R}x_2\oplus\cdots\oplus\boldsymbol{R}x_m\oplus\boldsymbol{R}x_{m+1}\oplus\cdots\oplus\boldsymbol{R}x_n \\ &=M'\oplus\boldsymbol{R}x_{m+1}\oplus\cdots\oplus\boldsymbol{R}x_n \end{aligned}$$

が成り立って，M'はMの直和因子である．

R-加群Mが部分加群 $M_1, M_2, \cdots, M_n$ の内部直和であるとき，Mの任意の元 x は $x=x_1+x_2+\cdots+x_n$ $(x_i\in M_i, 1\leqq i\leqq n)$ と一意的にあらわされる．したがって，写像

$$p_i\colon M\to M_i, \quad x\to x_i$$

は一意写像であり，また全射 R-準同型でもある．この p_i をMから M_i への **i-射影**とよぶ．

Mから M_i への i-射影 p_i に対して，M_i からMへの包含写像

$$\nu_i\colon M_i\to M, \quad x_i\to x_i$$

を **i-入射**とよぶ．ν_i は一意写像であり，単射 R-準同型である．p_i と ν_i との間には

$$p_i\circ\nu_i=1_{M_i}, \quad p_i\circ\nu_j=0 \quad (i\neq j)$$

の関係がある．M_i の元 x_i を

$$x_i=0+\cdots+0+\overset{i}{\breve{x_i}}+0+\cdots+0$$

とかきなおしてMの元とみれば，上の関係が成り立つことは明らかである．

Mの任意の元 $x=x_1+x_2+\cdots+x_n$ に対して

$$\textstyle\sum_{i=1}^n \nu_i(p_i(x))=\sum_{i=1}^n \nu_i(x_i)=\sum_{i=1}^n x_i=x$$

が成り立つから

$$\textstyle\sum_{i=1}^n \nu_i\circ p_i=1_M$$

でもある．

次の補題はしばしば有用である．

補題 3.5 M, N を R-加群とする．R-準同型 $f: M \to N$ に対して，R-準同型 $g: N \to M$ が存在して $fg = 1_N$ ならば，

$$M = (\mathrm{Ker}\, f) \oplus g(N).$$

証明 3.2 節でのべたように $\mathrm{Ker}\, f, g(N)$ 共に M の部分加群である．M の任意の元 x に対して，$x - gf(x) \in M$ で

$$f(x - gf(x)) = f(x) - fgf(x) = f(x) - f(x) = 0.$$

したがって，$x - gf(x) \in \mathrm{Ker}\, f$.

$x - gf(x) = y$ ($y \in \mathrm{Ker}\, f$) とおけば，$x = y + gf(x)$ で M は $\mathrm{Ker}\, f$ と $g(N)$ との和である．

一方，$(\mathrm{Ker}\, f) \cap g(N)$ の任意の元 $g(z)$ ($z \in N$) に対して

$$0 = f(g(z)) = fg(z) = z$$

であるから $(\mathrm{Ker}\, f) \cap g(N) = \{0\}$．したがって，$M$ は $\mathrm{Ker}\, f$ と $g(N)$ の内部直和である．

例 3 M, N を R-加群，$f: M \to N$ を R-準同型とする．M の部分加群 M' があって f の M' への制限写像 $f' = f|_{M'}: M' \to N$ が全単射ならば，

$$M = (\mathrm{Ker}\, f) \oplus M'.$$

仮定から N の任意の元は，ただ 1 個の M' の元 x' があって，$f'(x')$ とあらわされるので，写像 $g: N \to M'$ を $f'(x') \to x'$ ときめて，R-準同型 g がつくれる．

$$f(g(f'(x'))) = f(x') = f'(x')$$

から $fg = 1_N$ である．その上 $g(N) = M'$ であるから，補題 3.5 を用いて M は $\mathrm{Ker}\, f$ と M' の内部直和となる．

内部直和に対して外部直和を次のようにきめる．

$M_1, M_2, \cdots, M_n$ を R-加群とする（ある R-加群の部分加群とはかぎらない）．

$M_1, M_2, \cdots, M_n$ の直積集合

$$M_1 \times M_2 \times \cdots \times M_n = \{(x_1, x_2, \cdots, x_n) \mid x_1 \in M_1, x_2 \in M_2, \cdots, x_n \in M_n\}$$

に加法と R の元の作用を

$$(x_1, x_2, \cdots, x_n) + (y_1, y_2, \cdots, y_n) = (x_1 + y_1, x_2 + y_2, \cdots, x_n + y_n),$$
$$a \cdot (x_1, x_2, \cdots, x_n) = (ax_1, ax_2, \cdots, ax_n)$$

ときめると，$M_1 \times M_2 \times \cdots \times M_n$ は R-加群となる．こうしてできた R-加群を $M_1, M_2, \cdots, M_n$ の**外部直和**といい，内部直和と区別せずに同じ記号

$$M_1 \oplus M_2 \oplus \cdots \oplus M_n = \oplus_{i=1}^{n} M_i$$

であらわす．

このとき，各 i に対して，写像

$$p_i\colon M_1\oplus M_2\oplus\cdots\oplus M_n\to M_i,\quad (x_1,x_2,\cdots,x_n)\to x_i$$

を i–**射影**，写像

$$\nu_i\colon M_i\to M_1\oplus M_2\oplus\cdots\oplus M_n,\quad x_i\to(0,\cdots,0,\overset{i}{\breve{x_i}},0,\cdots,0)$$

を i–**入射**とよぶ．R–加群の演算のきめ方から p_i は全射 R–準同型であり，ν_i は単射 R–準同型である．

p_i と ν_i の間には，内部直和のときと同じように

$$\textstyle\sum_{i=1}^n \nu_i\circ p_i=1_M,\quad p_i\circ\nu_i=1_{M_i},\quad p_i\circ\nu_j=0\quad(i\neq j)$$

が成り立つ．

$M_1, M_2,\cdots,M_n$ を R–加群とし，その外部直和を M とおく．i–入射

$$\nu_i\colon M_i\to M,\quad x_i\to(0,\cdots,0,\overset{i}{\breve{x_i}},0,\cdots,0)$$

は単射 R–準同型であり，したがって，ν_i の像 $\nu_i(M)$ は M の部分加群となり，M_i に R–同型である．

M の任意の元 $x=(x_1,x_2,\cdots,x_n)$ は

$$\begin{aligned}x&=(x_1,0,\cdots,0)+(0,x_2,0,\cdots,0)+\cdots+(0,\cdots,0,x_n)\\&=\nu_1(x_1)+\nu_2(x_2)+\cdots+\nu_n(x_n)\end{aligned}$$

であるから，M は部分加群 $\nu_1(M_1),\nu_2(M_2),\cdots,\nu_n(M_n)$ の和である．

その上，$\nu_i(M_i)\cap\sum_{j\neq i}\nu_j(M_j)$ の任意の元 $\nu_i(x_i)=\sum_{j\neq i}\nu_j(x_j)$ は移項して $\sum_{j\neq i}\nu_j(x_j)-\nu_i(x_i)=0$ とかきなおせば，

$$(x_1,x_2,\cdots,x_{i-1},-x_i,x_{i+1},\cdots,x_n)=0$$

を意味するから，$x_i=0, \nu_i(x_i)=0$ となって $\nu_i(M_i)\cap\sum_{j\neq i}\nu_j(M_j)=\{0\}$ をうる．すなわち，

> R–加群 $M_1,M_2,\cdots,M_n$ の外部直和 M は $M_1,M_2,\cdots,M_n$ にそれぞれ R–同型な M の部分加群 $\nu_1(M_1),\nu_2(M_2),\cdots,\nu_n(M_n)$ の内部直和と一致する．

例 4　3.1 節例 4 の R–加群 R^n はそのつくり方から n 個の同じ R–左加群 R の外部直和である．3.1 節例 8 では，i–入射 ν_i の像 $\nu_i(R^n)$ を R_i であらわし，R^n が部分加群 $R_1,R_2,\cdots,R_n$ の和に等しいことを示したが，R^n は $R_1,R_2,\cdots,R_n$ の内部直和である．

逆に，M を R–加群，$M_1,M_2,\cdots,M_n$ を M の部分加群とし，M が $M_1,M_2,$

$\cdots, M_n$ の内部直和とする．$M_1, M_2, \cdots, M_n$ は M の部分加群であるが，R-加群でもあるから $M_1, M_2, \cdots, M_n$ の外部直和がつくれる．それを $M_1 \oplus M_2 \oplus \cdots \oplus M_n$ とかく．このとき写像

$$M_1 \oplus M_2 \oplus \cdots \oplus M_n \to M, \quad (x_1, x_2, \cdots, x_n) \to x_1 + x_2 + \cdots + x_n$$

は一意写像であり，R-同型でもある．したがって，この同型を同一視すれば内部直和は外部直和と一致する．この意味で内部直和，外部直和を区別しないで同じ記号であらわしてきた．それが内部直和をあらわすか，それとも外部直和をあらわすかは前後の関係から分かる．

例 5 ガウスの整数環 $\boldsymbol{Z}[i]$ は $\boldsymbol{C}$ の部分環であった (2.1 節例 10)．$\boldsymbol{Z}[i]$ を自然に $\boldsymbol{Z}$-加群にみることができる．このとき，写像

$$\boldsymbol{Z}[i] \to \boldsymbol{Z}, \quad a + bi \to a + b$$

は一意写像であり，全射 $\boldsymbol{Z}$-準同型であるが単射ではない．2つの $\boldsymbol{Z}$-(左)加群 $\boldsymbol{Z}$ の外部直和 $\boldsymbol{Z} \oplus \boldsymbol{Z}$ に対して写像

$$\boldsymbol{Z}[i] \to \boldsymbol{Z} \oplus \boldsymbol{Z}, \quad a + bi \to (a, b)$$

は $\boldsymbol{Z}$-同型である．同じようにして $\boldsymbol{R}$-加群とみて

$$\boldsymbol{C} \cong \boldsymbol{R} \oplus \boldsymbol{R}$$

が成り立つ．

3.4 自由加群

M を R-加群とする．ベクトル空間の場合と同じように，有限個の M の元 $x_1, x_2, \cdots, x_n$ が

$$a_1, a_2, \cdots, a_n \text{ が } R \text{ の元で } a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = 0$$
$$\Rightarrow a_1 = a_2 = \cdots = a_n = 0$$

であるとき，$x_1, x_2, \cdots, x_n$ は R 上 **1 次独立**であるという．R の上ということがはっきりしているときは，単に1次独立とよぶ．

無限個の M の元は，その中の有限個の元がすべて1次独立であるとき，1次独立ときめる．

1次独立な生成元をもつ R-加群を自由 R-加群または単に**自由加群**とよぶ．自由加群の1次独立な生成元を**基底**とよぶ．これもベクトル空間の場合と同じである．基底はかならずしも一意的にはきまらない．

便宜上零加群は自由加群であるときめる．

例 1 $\boldsymbol{R}$ の上のベクトル空間は自由 $\boldsymbol{R}$-加群である．

例 2　環RをR-加群とみたとき，Rは単位元1を基底とする自由加群である．RはまたRの任意の単元を基底とする自由加群でもある．

例 3　3.1節例8で，$e_1, e_2, \cdots, e_n$がR^nの生成元であることをのべた．$a_1, a_2, \cdots, a_n \in R$で$a_1e_1+a_2e_2+\cdots+a_ne_n=0$ならば，

$$(a_1, a_2, \cdots, a_n)=a_1e_1+a_2e_2+\cdots+a_ne_n$$

であるから，$a_1=a_2=\cdots=a_n=0$で$e_1, e_2, \cdots, e_n$はR上1次独立でもあり，R^nは$e_1, e_2, \cdots, e_n$を基底とする自由加群である．

例 4　$R=\boldsymbol{Z}/(n)$（nは自然数）はR-加群とみて自由加群であったが，$\boldsymbol{Z}$-加群とみては自由加群ではない．

実際，Rのどんな元もn倍すると0になるから，Rのどんな部分集合も$\boldsymbol{Z}$上1次独立とはなりえない．

自由加群はベクトル空間と類似の性質をもつ．しかし，ベクトル空間とは斜体または体の上の自由加群であるのに対して，自由加群はかならずしも斜体または体とはかぎらない一般の環の上の自由加群である．

例えば，よく知られたように，ベクトル空間では生成元の中から基底をとりだすことができるが，自由加群ではこのことは一般には成り立たない．

$\boldsymbol{Z}$-加群$\boldsymbol{Z}$は自由加群であり，後で定理3.8で示すように，その基底の個数はいつも1である．しかし，3.1節例9で示したように2, 3は$\boldsymbol{Z}$の生成元であるが，この中から$\boldsymbol{Z}$の基底をとりだすことはできない．

もう一つ，ベクトル空間では成り立っても，一般の自由加群では成り立たないことをあげよう．

ベクトル空間の元$x_1, x_2, \cdots, x_n$が1次独立でないならば，この中のあるx_iは残りの元の1次結合としてあらわされる．この性質も一般の自由加群では成り立たない．

例えば，2, 3は$\boldsymbol{Z}$上1次独立ではない．このことは$2\cdot(-3)+3\cdot 2=0$から分かる．しかし，$2=3\cdot a$または$3=2\cdot b$をみたす整数a, bは存在しない．

定理 3.6　R-加群Mの元$x_1, x_2, \cdots, x_n$に対して，次の条件は同値である．

(1)　Mは$x_1, x_2, \cdots, x_n$を基底とする自由加群である．

(2)　Mの各元xは

$$x=a_1x_1+a_2x_2+\cdots+a_nx_n \qquad (a_i \in R, 1 \leqq i \leqq n)$$

の形にあらわされ，その上，もし

$$x=a_1x_1+a_2x_2+\cdots+a_nx_n=b_1x_1+b_2x_2+\cdots+b_nx_n \qquad (a_i, b_i \in R)$$

と二通りにあらわされるならば,

$$a_1=b_1,\quad a_2=b_2,\quad \cdots,\quad a_n=b_n.$$

(3) $x_1, x_2, \cdots, x_n$ の左零化イデアルはすべて $\{0\}$ で,

$$M=Rx_1\oplus Rx_2\oplus\cdots\oplus Rx_n.$$

証明 (1) ⇒ (2) は 3.3 節例 1 の証明と同じようにしてできる.

(2) ⇒ (3): (2) の前半にのべたことから, M の各元 x は

$$x=a_1x_1+a_2x_2+\cdots+a_nx_n \qquad (a_i\in R)$$

の形にあらわされる. (2) の後半にのべたことから, x がもし

$$x=a_1x_1+a_2x_2+\cdots+a_nx_n=b_1x_1+b_2x_2+\cdots+b_nx_n \qquad (a_i, b_i\in R)$$

と二通りにあらわされるならば, $a_1=b_1, a_2=b_2, \cdots, a_n=b_n$. したがって,

$$a_1x_1=b_1x_1, a_2x_2=b_2x_2, \cdots, a_nx_n=b_nx_n$$

となって, x は

$$x=a_1x_1+a_2x_2+\cdots+a_nx_n$$

の形に一意的にあらわされる. 定理 3.4 から

$$M=Rx_1\oplus Rx_2\oplus\cdots\oplus Rx_n.$$

x_i の左零化イデアル $\mathrm{Ann}_R\, x_i$ から元 a をとる. a は R の元で $ax_i=0$ をみたす. これを

$$\begin{aligned}&0\cdot x_1+0\cdot x_2+\cdots+0\cdot x_{i-1}+ax_i+0\cdot x_{i+1}+\cdots+0\cdot x_n\\&=0\cdot x_1+0\cdot x_2+\cdots+0\cdot x_n\end{aligned}$$

と考えれば, あらわし方の一意性から $a=0$ をうる.

(3) ⇒ (1): (3) の後半から $x_1, x_2, \cdots, x_n$ は M の生成元である. $x_1, x_2, \cdots, x_n$ が R 上 1 次独立であることを示す. $a_1, a_2, \cdots, a_n$ が R の元で $a_1x_1+a_2x_2+\cdots+a_nx_n=0$ ならば, あらわし方の一意性から

$$a_1x_1=a_2x_2=\cdots=a_nx_n=0.$$

(3) の前半から $x_1, x_2, \cdots, x_n$ の左零化イデアルはすべて $\{0\}$ で

$$a_1=a_2=\cdots=a_n=0$$

をうる. すなわち, $x_1, x_2, \cdots, x_n$ は R 上 1 次独立である.

M を R-加群, $x_1, x_2, \cdots, x_n$ を M の元とする. このとき写像

$$\alpha\colon R^n\to M,\quad (a_1, a_2, \cdots, a_n)\to \textstyle\sum_{i=1}^n a_ix_i$$

は一意写像であり, R-準同型にもなっている (3.2 節例 6).

定理 3.7 M を R-加群とし, M の元 $x_1, x_2, \cdots, x_n$ に対して, 上のように R-準同型 α をきめる. このとき次の条件は同値である.

(1)　Mは$x_1, x_2, \cdots, x_n$を基底とする自由加群である．

(2)　$\alpha: R^n \to M$はR-同型である．

(3)　任意のR-加群N, 任意のNの元$y_1, y_2, \cdots, y_n$に対して，$f(x_i)=y_i$ $(1 \leqq i \leqq n)$をみたすR-準同型$f: M \to N$がただ1つ存在する．

証明　(1) ⇒ (2)：$x_1, x_2, \cdots, x_n$がMの生成元であるからαは全射であり，$x_1, x_2, \cdots, x_n$が1次独立であるからαは単射である．

(2) ⇒ (3)：αが全射であるから，Mの任意の元xは適当なR^nの元$(a_1, a_2, \cdots, a_n)$によって$x=\alpha((a_1, a_2, \cdots, a_n))=\sum_{i=1}^n a_i x_i$とかける．このとき

$$f: M \to N, \quad x \to \sum_{i=1}^n a_i y_i$$

とfをきめたらよい．fが一意写像であることはαが単射であることから分かる．fがR-準同型であることも明らかである．

もし$f, f': M \to N$が共にR-準同型で各iに対して$f(x_i)=y_i=f'(x_i)$であるならば，Mの任意の元xが$x=\sum_{i=1}^n a_i x_i$とあらわされるから

$$f(x)=\sum_{i=1}^n a_i \cdot f(x_i)=\sum_{i=1}^n a_i \cdot f'(x_i)=f'(x)$$

となり，$f=f'$をうる．

(3) ⇒ (1)：(3)でNをR^nに，y_iをe_iにとれば，仮定から$f(x_i)=e_i$をみたすR-準同型$f: M \to R^n$が（ただ1つ）存在する．

次に，(3)でNをMとし，y_iをx_iにとれば，仮定からx_iをx_iにうつすR-準同型$M \to M$がただ1つ存在する．ところで，各iに対して

$$\alpha(f(x_i))=\alpha(e_i)=x_i, \quad 1_M(x_i)=x_i$$

であり，$\alpha f, 1_M$共にMからMへのR-準同型であるから

$$\alpha f=1_M$$

が成り立つ．ここで1_MはMの恒等写像をあらわす．

このことから，特に，αは全射であり，Mの任意の元xは$x=\sum_{i=1}^n a_i x_i$とかける．$x_1, x_2, \cdots, x_n$はMの生成元である．

$x_1, x_2, \cdots, x_n$が1次独立であることを示す．$a_1, a_2, \cdots, a_n$がRの元で$\sum_{i=1}^n a_i x_i=0$ならば，

$$0=f\left(\sum_{i=1}^n a_i x_i\right)=\sum_{i=1}^n a_i e_i=(a_1, a_2, \cdots, a_n)$$

であるから，$a_1=a_2=\cdots=a_n$となる．

例 5　MをR-加群としMの元$x_1, x_2, \cdots, x_n$をとって，上のように$\alpha: R^n \to M$を考える．このとき定理3.7の証明からも分かるように

$$\alpha \text{が全射} \Leftrightarrow x_1, x_2, \cdots x_n \text{が} M \text{の生成元}$$

であるから

$$M\text{が有限生成加群} \Leftrightarrow \text{ある}\, n>0\, \text{と}\, M\, \text{の元}\, x_1, x_2, \cdots, x_n\, \text{が}$$
$$\text{あって}\, \alpha\, \text{が全射}$$

も成り立つ(3.2節例6).

例 6 Rが可換環，AがRの $\{0\}$ でないイデアルならば，

$$A\text{が自由加群} \Leftrightarrow \text{零因子でない}\, R\, \text{の元}\, a\, \text{があって}\, A=Ra.$$

実際，零因子でないRの元はR上1次独立であるから $\Leftarrow$ は明らか．$\Rightarrow$ を示すために，Aが自由加群ならば，その基底はただ1個の元からなることを確かめる．Aの基底が2個以上の元をもつとし，その中の2元をa, bとする．a, bはR上1次独立であり，しかも $ba+(-a)b=0$ であるから $b=-a=0$ でなければならない．零元は1次独立ではありえないから矛盾である．したがって，Aの基底はただ1個の元からなり，それをaとかけば$A=Ra$である．aは1次独立であるから零因子ではありえない．

例 7 Rが可換環のとき

$$R\text{が単項イデアル整域} \Leftrightarrow R\text{のイデアルはすべて自由加群}.$$

$\Rightarrow$ は例6による．$\Leftarrow$ は，Rのイデアルがすべて単項イデアルであることは例6によって分かるから，Rが零因子をもたないことを示せばよい．$R\ni a$ $(\neq 0)$ がRの零因子とする．Raは $\{0\}$ でないRのイデアルであるから，例6により，零因子ではないRの元bがあって$Ra=Rb$とかける．$b=ca$とかけば，aが零因子であるからbも零因子となって矛盾である．

例 8 　環Rが斜体 $\Leftrightarrow$ R-加群はすべて自由加群.

$\Rightarrow$ は，$\boldsymbol{R}$にかぎらず斜体Rの上の $\{0\}$ でない左ベクトル空間は基底をもち，したがって，自由加群である．$\Leftarrow$ を示すために，Mを単純R-加群とする．仮定からMは自由加群で，Mの基底の中から1元xをとれば$M=Rx$であり，かつ，xはR上1次独立である．したがって，R-準同型α: $R\to M$, $a\to ax$はR-同型で${}_RR$は単純加群となる．3.1節例7からRは斜体である．

例 9 $\boldsymbol{Z}$は単項イデアル整域であるから，イデアルはすべて$\boldsymbol{Z}$-加群とみて自由加群である(例7)が，$\boldsymbol{Z}$は斜体でないから，自由加群でない$\boldsymbol{Z}$-加群が存在する(例8)．例えば，$\{0\}$ でない有限加法群は$\boldsymbol{Z}$-加群とみて自由加群ではなかった(例4)．また，$\boldsymbol{Q}$も$\boldsymbol{Z}$-加群とみて自由加群ではない．

実際，$\boldsymbol{Q}$が$\boldsymbol{Z}$-加群とみて自由加群とするとき，基底が1元のみということはありえないし，$\boldsymbol{Q}$の2個以上の元が$\boldsymbol{Z}$上1次独立にはなりえないから，いずれにしても矛盾がおこる．詳しい証明は演習問題とする．

一般に自由加群の基底が一通りではないことを例2でのべたが，基底をつくる元の個数については次の定理が成り立つ．

定理 3.8　Rを可換環，Mを$x_1, x_2, \cdots, x_n$を基底とする自由R-加群とする．このとき，基底の元の個数nは基底のとり方によらず一定である．

証明　AをRの極大イデアルとする（補題3.3）．各iに対して，$Ax_i=\{ax_i | a\in A\}$はMの部分加群である．

$$AM=Ax_1+Ax_2+\cdots+Ax_n$$

とおく．

剰余加群M/AMはR-加群であるが，剰余環R/Aの上の加群とみることもできる．それには$M/AM\ni x+AM, R/A\ni a+A$に対して

$$(a+A)\cdot(x+AM)=ax+AM$$

ときめたらよい．R/Aは体（3.1節例7）であるから，M/AMは体R/Aの上のベクトル空間である．

$M=Rx_1+Rx_2+\cdots+Rx_n$から

$$M/AM=R/A\cdot(x_1+AM)+\cdots+R/A\cdot(x_n+AM)$$

が成り立ち，$x_1+AM, x_2+AM, \cdots, x_n+AM$は$M/AM$の生成元である．

$x_1+AM, x_2+AM, \cdots, x_n+AM$が$R/A$上1次独立であることを示す．$a_1+A, a_2+A, \cdots, a_n+A$が$R/A$の元で

$$(a_1+A)\cdot(x_1+AM)+\cdots+(a_n+A)\cdot(x_n+AM)=0+AM$$

ならば，$a_1x_1+a_2x_2+\cdots+a_nx_n+AM=0+AM$であるから

$$a_1x_1+a_2x_2+\cdots+a_nx_n\in AM=Ax_1+Ax_2+\cdots+Ax_n.$$

適当なAの元$b_1, b_2, \cdots, b_n$があって$a_1x_1+a_2x_2+\cdots+a_nx_n=b_1x_1+b_2x_2+\cdots+b_nx_n$であるが，$x_1, x_2, \cdots, x_n$は$R$上1次独立であるから

$$a_1=b_1, a_2=b_2, \cdots, a_n=b_n.$$

したがって，$a_1, a_2, \cdots, a_n$はすべてAに属し

$$a_1+A=0+A,\ \ a_2+A=0+A, \cdots, a_n+A=0+A.$$

すなわち，$x_1+AM, x_2+AM, \cdots, x_n+AM$は$M/AM$の$R/A$上の基底である．体の上のベクトル空間の基底をつくる元の個数は，基底のとり方によらず一定であるから，nはMの基底のとり方によらず一定である．

自由加群Mの基底をつくる元の個数が一定であるとき，この一定の値をMの**階数**とよぶ．便宜上零加群は自由加群ときめたが，その階数は0とする．

自由 R-加群が無限個の元からなる基底をもてば，（R が可換環でなくても）基底をつくる元の濃度が一定であることを一般に証明できるが，ここでは触れない．また，可換でない環の上の自由加群では，任意有限個の元からなる基底をもつものがあることも知られているが，これもここでは触れない．

3.5　アーベル群の基本定理（1）

この節と次の節では単項イデアル整域Rの上の加群の構造定理をのべ，その特別な場合として，いわゆるアーベル群の基本定理を証明する．

定理 3.9　可換環Rに対して，次の条件は同値である．

(1)　Rは単項イデアル整域である．

(2)　Rのイデアルはすべて自由加群である．

(3)　階数有限の自由加群Mの部分加群Nも自由加群であり，その階数はMの階数をこえない．

証明　(1) と (2) の同値は 3.4 節例 7 でのべた．(3) $\Rightarrow$ (2) は明らかであるから (2) $\Rightarrow$ (3) を示せばよい．

Mを階数有限の自由加群，Nをその $\{0\}$ ではない部分加群とする．Mの基底を $x_1, x_2, \cdots, x_m$ とおき，mに関する帰納法で，Nも自由加群であり，その階数がmをこえないことを示す．

$m=1$ のときは $M=Rx_1$ であり，Rx_1 はRと R-同型であるから，NはRの $\{0\}$ でないイデアルAと R-同型である．仮定からAは自由加群で，零因子でないRの元 a があって $A=Ra$ とかける（3.4 節例 6）．a はR上 1 次独立であるからAの階数は 1 であり，Aと R-同型なNもまた階数 1 の自由加群である．

$m>1$ とし，階数 $m-1$ の自由加群に対しては (3) が成り立つものと仮定する．$M=Rx_1\oplus Rx_2\oplus\cdots\oplus Rx_m$ であり（定理 3.6），各 i に対して写像f_iを

$$f_i\colon M\to R,\quad x=\sum_{i=1}^m a_ix_i\to a_i$$

ときめる．f_i は一意写像であり，R-準同型でもある．

Nは 0 でない元 x を含む．この x に対して $f_i(x)\neq 0$ なる i がある．必要ならば番号をつけかえて $f_1(x)\neq 0$ とする．このとき $f_1(N)$ はRの $\{0\}$ でないイデアルで，零因子でないRの元 d があって $f_1(N)=Rd$ とかける．

$f_1(y)=d$ となるNの元 y をとり，写像 g を

$$g\colon Rd\to N,\quad ad\to ay$$

ときめれば，g は一意写像であり，R-準同型でもある．

f_1 の N への制限写像 $f_1|_N$ を f_1' とかけば，

$$f_1'(g(ad))=f_1'(ay)=a\cdot f_1'(y)=ad$$

となって $f_1'g=1_{Rd}$ をうる．補題3.5から

$$N=(\mathrm{Ker}\, f_1')\oplus g(Rd).$$

このとき $\mathrm{Ker}\, f_1'=(\mathrm{Ker}\, f_1)\cap N\subseteqq \mathrm{Ker}\, f_1=\oplus_{i=2}^m Rx_i$ であるから，$\mathrm{Ker}\, f_1'$ は階数 $m-1$ の自由加群 $\oplus_{i=2}^m Rx_i$ の部分加群として帰納法の仮定から自由加群でありその階数は $m-1$ をこえることはない．

一方，$f_1'g=1_{Rd}$ から g は単射であり，$g(Rd)\cong Rd\cong R$ であるから $g(Rd)$ は階数1の自由加群である．

したがって，$N=(\mathrm{Ker}\, f_1')\oplus g(Rd)$ は自由加群でその階数は m をこえない．

R-加群 M に対して，M から R への R-準同型の全体 $\mathrm{Hom}_R(M, R)$ を M^* とかく．M^* の2元 f, g の和 $f+g$ を

$$f+g\colon M\to R,\quad x\to f(x)+g(x)$$

ときめて，M^* を加法群にすることができる(3.2節参照)．M^* の零元は M のすべての元を R の零元にうつす M から R への写像であり，M^* の元 f の逆元は M の各元 x を $-f(x)$ にうつす M から R への写像である．

その上，$M^*\times R$ から M^* への写像 $(f, a)\to fa$ を

$$fa\colon M\to R,\quad x\to f(x)\cdot a$$

ときめて，M^* を R-右加群にできる．詳しい証明は演習問題とする．この M^* を M の**双対加群**とよぶ．

特に M を自由 R-加群，$x_1, x_2, \cdots, x_m$ をその基底とする．定理3.9の証明でのべた R-準同型

$$f_i\colon M\to R,\quad x=\sum_{i=1}^m a_ix_i\to a_i$$

は M^* の元である．

$x\in M$ とする．$x\neq 0$ ならば，$x=\sum_{i=1}^m a_ix_i$ においてある i があって a_i は0ではない．したがって，$f_i(x)\neq 0$．すなわち，

$$x=0 \Leftrightarrow \text{すべての } f\in M^* \text{ に対して } f(x)=0$$

が成り立つ．

例 1　R-左加群 R の双対加群 R^* は R-右加群 R と R-同型である．

写像 $\alpha\colon R^*\to R$ を $f\to f(1)$ ときめる．α は一意写像であり R-準同型であ

る．$f, g \in R^*$ に対して $f(1)=g(1)$ ならば，R の任意の元 a に対して $f(a)=a\cdot f(1)=a\cdot g(1)=g(a)$ が成り立つから $f=g$ で，α は単射である．

R の任意の元 b に対して，$f: R \to R$，$a \to ab$ ときめれば $f \in R^*$ で $f(1)=b$ であるから，α は全射である．

例 2 $\boldsymbol{Z}$-加群とみたとき，$\boldsymbol{Q}$ の双対加群 $\boldsymbol{Q}^*$ は $\{0\}$ である．この証明は演習問題とする．

有限次元ベクトル空間では，部分空間の任意の基底をひろげてもとの空間の基底をつくることができる．定理 3.9 によれば，R が単項イデアル整域であるとき，階数有限の自由加群 M の $\{0\}$ でない部分加群 N も自由加群で基底をもつ．次の定理は M の適当な基底の中から N のある基底がつくれることを示している．まず，補題を準備する．

補題 3.10 単項イデアル整域 R のイデアルからなる空でない集合は極大元をもつ．

証明 $\mathcal{A}$ を，R のイデアルからなる空でない集合で，極大元をもたないものとする．$\mathcal{A}$ から 1 つ A_1 をとりだす．A_1 は $\mathcal{A}$ の極大元でないから $A_1 \subsetneqq A_2$ をみたす $\mathcal{A}$ の元 A_2 がある．A_2 も $\mathcal{A}$ の極大元でないから $A_2 \subsetneqq A_3$ をみたす $\mathcal{A}$ の元 A_3 がある．このようにして R のイデアルの無限列

$$A_1 \subsetneqq A_2 \subsetneqq A_3 \subsetneqq \cdots$$

ができて補題 2.20 に矛盾する．

定理 3.11 R を単項イデアル整域，M を階数 m の自由 R-加群，N を $\{0\}$ でない M の部分加群でその階数を $n\ (\leqq m)$ とする．このとき，M の基底 $x_1, x_2, \cdots, x_m$ と，R の 0 でない元 $a_1, a_2, \cdots, a_n$ とがあって

(1) $\{a_1x_1, a_2x_2, \cdots, a_nx_n\}$ は N の基底，

(2) $Ra_1 \supseteqq Ra_2 \supseteqq \cdots \supseteqq Ra_n$

となるようにすることができる．

証明 m に関する帰納法で証明する．$m=1$ のときは，定理 3.9 の証明で示したように，$\{0\}$ でない M の部分加群 N も階数 1 の自由加群である．M の基底を x_1 とかけば，$M=Rx_1$ であり，N の基底は a_1x_1 ($a_1 \in R$, $a_1 \neq 0$) の形をしている．

$m>1$ とし，階数 $m-1$ の自由加群に対しては定理が正しいものと仮定する．証明をいくつかの段階に分けてのべる．

(i) $\{g(N) \mid g \in M^*\}$ は R のイデアルからなる空でない集合で補題 3.10 か

ら極大元をもつ．この極大元を $g_1(N)$ とかき

$$g_1(N)=Ra_1, \qquad a_1=g_1(y_1), y_1\in N$$

とあらわす．

ここで a_1 は 0 ではない．実際，$a_1=0$ ならば，$g_1(N)=\{0\}$．しかし，N には 0 でない元 y があり，双対加群のところで注意したように，ある $g\in M^*$ があって $g(y)\neq 0$．この g に対しては

$$g(N)\neq\{0\}, \quad g_1(N)=\{0\}\subsetneqq g(N).$$

これは $g_1(N)$ の極大性に矛盾する．

(ii)　M^* の任意の元 g に対して $g(y_1)\in Ra_1$ を示す．

ある g に対して $g(y_1)\notin Ra_1$ とする．$Ra_1\subsetneqq Ra_1+R\cdot g(y_1)$ であり，$Ra_1+R\cdot g(y_1)=Rb$ $(b\in R)$ とかけば，$ca_1+d\cdot g(y_1)=b$ をみたす R の元 c, d が存在する．このとき，$g_1c+gd\in M^*$ で

$$(g_1c+gd)(y_1)=g_1(y_1)\cdot c+g(y_1)\cdot d=b.$$

したがって，$b\in(g_1c+gd)(N)$ となり

$$g_1(N)=Ra_1\subsetneqq Rb\subseteqq(g_1c+gd)(N).$$

これは $g_1(N)$ の極大性に反する．

(iii)　R 上 1 次独立な M の元 x_1 があって，M が

$$M=(\mathrm{Ker}\, g_1)\oplus Rx_1$$

と分解されることを示す．

M の基底を $u_1, u_2, \cdots, u_m$ とおき，各 i に対して写像 f_i を

$$f_i\colon M\to R, \quad \textstyle\sum_{i=1}^m b_iu_i\to b_i$$

ときめる．$f_i\in M^*$ で，したがって，(ii)から $f_i(y_1)=c_ia_1$ $(c_i\in R)$ とかける．

$$\begin{aligned} y_1&=f_1(y_1)\cdot u_1+f_2(y_1)\cdot u_2+\cdots+f_m(y_1)\cdot u_m \\ &=a_1\cdot(c_1u_1+c_2u_2+\cdots+c_mu_m). \end{aligned}$$

求める x_1 を $x_1=c_1u_1+c_2u_2+\cdots+c_mu_m$ ときめる．このとき

$$y_1=a_1x_1, \quad a_1=g_1(y_1)=g_1(a_1x_1)=a_1\cdot g_1(x_1).$$

R は整域で $a_1\neq 0$ であるから $g_1(x_1)=1$ となる．写像

$$h\colon R\to M, \quad a\to ax_1$$

は一意写像であり，R-準同型で

$$g_1(h(a))=g_1(ax_1)=a$$

から $g_1h=1_R$ (1_R は R の恒等写像) をみたす．補題 3.5 によって

$$M=(\mathrm{Ker}\, g_1)\oplus h(R)=(\mathrm{Ker}\, g_1)\oplus Rx_1.$$

x_1 が R 上 1 次独立であることは，R の元 a に対して $ax_1=0$ ならば

$$0=g_1(ax_1)=a\cdot g_1(x_1)=a$$

であることから分かる．

したがって，Rx_1 は階数 1 の自由加群であり，$m>1$ から $\mathrm{Ker}\, g_1$ は $\{0\}$ ではありえず，階数 $m-1$ の自由加群である(演習問題 42).

(iv)　N もまた

$$N=((\mathrm{Ker}\, g_1)\cap N)\oplus Ra_1x_1$$

と分解されることを示す．

N から任意の元 y をとる．$g_1(y)\in g_1(N)=Ra_1$ であるから，$g_1(y)=ca_1$ ($c\in R$) とかく．$y-cy_1\in N$ であり

$$g_1(y-cy_1)=g_1(y)-c\cdot g_1(y_1)=0$$

から $y-cy_1\in(\mathrm{Ker}\, g_1)\cap N$. $y_1=a_1x_1$ であったから

$$y=(y-cy_1)+cy_1\in((\mathrm{Ker}\, g_1)\cap N)+Ra_1x_1.$$

このことは $N=((\mathrm{Ker}\, g_1)\cap N)+Ra_1x_1$ を意味している．その上，$((\mathrm{Ker}\, g_1)\cap N)\cap Ra_1x_1\subseteqq(\mathrm{Ker}\, g_1)\cap Rx_1=\{0\}$ であるから，$N=((\mathrm{Ker}\, g_1)\cap N)\oplus Ra_1x_1$ となる．

(v)　$(\mathrm{Ker}\, g_1)\cap N=\{0\}$ のときは，$N=Ra_1x_1$ である．$\mathrm{Ker}\, g_1$ は階数 $m-1$ の自由加群，その基底を $x_2, x_3, \cdots, x_m$ とおく．このとき $x_1, x_2, \cdots, x_m$ は $M=(\mathrm{Ker}\, g_1)\oplus Rx_1$ の基底となる．a_1x_1 は R 上 1 次独立であるから N の基底をつくる．このときは定理の証明ができたことになる．

(vi)　$(\mathrm{Ker}\, g_1)\cap N\neq\{0\}$ のときは，帰納法の仮定から，$\mathrm{Ker}\, g_1$ の基底 $x_2, x_3, \cdots, x_m$ と R の 0 でない元 $a_2, a_3, \cdots, a_l$ ($l\leqq m$) があって

(1)　$\{a_2x_2, a_3x_3, \cdots, a_lx_l\}$ は $(\mathrm{Ker}\, g_1)\cap N$ の基底，

(2)　$Ra_2\supseteqq Ra_3\supseteqq\cdots\supseteqq Ra_l$

とできる．

このとき，$x_1, x_2, \cdots, x_m$ は M の基底であり，$a_1x_1, a_2x_2, \cdots, a_lx_l$ は $N=((\mathrm{Ker}\, g_1)\cap N)\oplus Ra_1x_1$ の基底となるから，$Ra_1\supseteqq Ra_2$ のみ示せばよい．

M の基底 $x_1, x_2, \cdots, x_m$ に関して，(iii)の f_i と同じような R-準同型

$$k_i\colon M\to R,\quad \textstyle\sum_{i=1}^m b_ix_i\to b_i$$

をつくる．特に，k_2 を用いて写像 k を

$$k\colon M=(\mathrm{Ker}\, g_1)\oplus Rx_1\to R,\quad x+b_1x_1\to k_2(x)+b_1$$

ときめる．ここで $x\in\mathrm{Ker}\, g_1$ とする．k は一意写像であり，R-準同型にもな

っている．したがって，$k\in M^*$ である．

$k(a_1x_1)=a_1$ は $a_1\in k(N)$ を意味し，$g_1(N)=Ra_1\subseteqq k(N)$ が成り立つが，$g_1(N)=Ra_1$ の極大性から $Ra_1=k(N)$.

一方，$k(a_2x_2)=k_2(a_2x_2)=a_2$ からは $a_2\in k(N)=Ra_1$ となり，$Ra_2\subseteqq Ra_1$ であることが分かる．

有限生成 R-加群の構造定理をのべるために，補題を準備する．

補題 3.12　M が R-加群で，その部分加群 $M_1, M_2, \cdots, M_m$ の内部直和とする．$i=1,2,\cdots,m$ に対して N_i が M_i の部分加群ならば，$M/\sum_{i=1}^m N_i$ は $\pi(M_1), \pi(M_2), \cdots, \pi(M_m)$ の内部直和であり，$\pi(M_i)\cong M_i/N_i$ が成り立つ．ここで π: $M\to M/\sum_{i=1}^m N_i$ は標準的 R-準同型をあらわす．

証明　$M/\sum_{i=1}^m N_i$ の任意の元を $\pi(x)$ $(x\in M)$ とかく．x は

$$x=x_1+x_2+\cdots+x_m \qquad (x_i\in M_i)$$

とあらわされるから $\pi(x)=\pi(x_1)+\pi(x_2)+\cdots+\pi(x_m)$ $(\pi(x_i)\in\pi(M_i))$.

もし $\pi(x)=\sum_{i=1}^m \pi(x_i)=\sum_{i=1}^m \pi(y_i)$ $(x_i, y_i\in M_i)$ と二通りにあらわされるならば，$\sum_{i=1}^m (x_i-y_i)\in \mathrm{Ker}\,\pi=\sum_{i=1}^m N_i$. したがって，

$$\sum_{i=1}^m (x_i-y_i)=\sum_{i=1}^m z_i \qquad (z_i\in N_i)$$

とあらわせば $\sum_{i=1}^m (x_i-y_i-z_i)=0$. M が $M_1, M_2, \cdots, M_m$ の内部直和であるから各 i に対して

$$x_i-y_i-z_i=0, \quad x_i=y_i+z_i.$$

$z_i\in N_i\subseteqq \mathrm{Ker}\,\pi$ から，$\pi(x_i)=\pi(y_i)$ となる．$\pi(x)$ は

$$\pi(x)=\pi(x_1)+\pi(x_2)+\cdots+\pi(x_m)$$

と一意的にあらわされる．その上

$$\pi(M_i)=\left(M_i+\sum_{i=1}^m N_i\right)\Big/\sum_{i=1}^m N_i\cong M_i\Big/\left(M_i\cap\sum_{i=1}^m N_i\right)=M_i/N_i.$$

定理 3.13（有限生成加群の構造定理）　R を単項イデアル整域とすれば，有限生成 R-加群 M は有限個の巡回加群の直和として

$$M\cong(\oplus_{i=1}^n R/Ra_i)\oplus R^s$$

の形にあらわされる．ここで $a_1, a_2, \cdots, a_n$ は

$$R\neq Ra_1\supseteqq Ra_2\supseteqq\cdots\supseteqq Ra_n\neq\{0\}$$

をみたす．

証明　$M=Rx_1+Rx_2+\cdots+Rx_m$ とする．写像

$$\alpha\colon R^m\to M, \quad (a_1, a_2, \cdots, a_m)\to\sum_{i=1}^m a_ix_i$$

は全射 R-準同型で(3.2節例6)，図3.6の図型は可換となる．ここで π は標準的な R-準同型，$\bar{\alpha}$ は α から誘導された R-同型である．

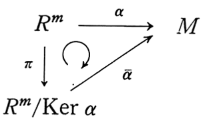


図 3.6

$\mathrm{Ker}\,\alpha=\{0\}$ のときは $M\cong R^m$ である．

$\mathrm{Ker}\,\alpha\neq\{0\}$ のときは，R^m の基底 $u_1, u_2, \cdots, u_m$ と R の 0 でない元 $a_1, a_2, \cdots, a_n$ があって

$$\{a_1u_1, a_2u_2, \cdots, a_nu_n\} \text{ は } \mathrm{Ker}\,\alpha \text{ の基底で，} Ra_1\supseteqq Ra_2\supseteqq\cdots\supseteqq Ra_n$$

とすることができる(定理3.11)．

$$R^m=Ru_1\oplus Ru_2\oplus\cdots\oplus Ru_m$$
$$\mathrm{Ker}\,\alpha=Ra_1u_1\oplus Ra_2u_2\oplus\cdots\oplus Ra_nu_n$$

で，Ra_iu_i は Ru_i の部分加群であり，$\{0\}$ も Ru_i の部分加群とみて補題3.12を適用すれば，

$$R^m/\mathrm{Ker}\,\alpha=\pi(Ru_1)\oplus\pi(Ru_2)\oplus\cdots\oplus\pi(Ru_m),$$
$$(\pi(Ru_i)\cong Ru_i/Ra_iu_i \quad (1\leqq i\leqq n), \quad \pi(Ru_i)\cong Ru_i \quad (n+1\leqq i\leqq m)).$$

$u_1, u_2, \cdots, u_m$ が基底であるから写像

$$R/Ra_i \to Ru_i/Ra_iu_i, \quad a+Ra_i \to au_i+Ra_iu_i \qquad (1\leqq i\leqq n),$$
$$R \to Ru_i, \qquad a \to au_i \qquad (n+1\leqq i\leqq m)$$

は共に R-同型，したがって，

$$M\cong R^m/\mathrm{Ker}\,\alpha\cong(\oplus_{i=1}^n R/Ra_i)\oplus R^{m-n}.$$

Ra_i の中に R に等しいものがあれば，それを除いて

$$R\neq Ra_1\supseteqq Ra_2\supseteqq\cdots\supseteqq Ra_n\neq\{0\}$$

と考えてよい．

定理3.13の直和分解は一意的であるが，これは次の節で示す．ここでは，次の節のための準備を続ける．次の補題は Chinese Remainder Theorem とよばれている．

補題 3.14　R を環，$A_1, A_2, \cdots, A_n$ を R のイデアルで $i\neq j$ ならば，

$$R=A_i+A_j$$

であるとする．このとき，R から剰余環 $R/A_1, R/A_2, \cdots, R/A_n$ の直積 $\prod_{i=1}^n R/A_i = R/A_1 \times R/A_2 \times \cdots \times R/A_n$ への写像

$$f\colon R \to \prod_{i=1}^n R/A_i, \quad a \to (a+A_1, a+A_2, \cdots, a+A_n)$$

は全射環準同型，その核は $\bigcap_{i=1}^n A_i$ で，したがって，

$$R/\bigcap_{i=1}^n A_i \cong^{\bar{f}} \prod_{i=1}^n R/A_i.$$

証明　仮定の $R=A_i+A_j$ $(i \neq j)$ から $R=A_i+\bigcap_{j\neq i} A_j$ が成り立つ（この証明は演習問題とする）．各 i に対して，$R=A_i+\bigcap_{j\neq i} A_j$ から

$$1=b_i+b_i' \qquad (b_i \in A_i,\ b_i' \in \bigcap_{j\neq i} A_j)$$

とおく．$\prod_{i=1}^n R/A_i$ の任意の元 $(a_1+A_1, a_2+A_2, \cdots, a_n+A_n)$ をとり R の元 a を

$$a=b_1'a_1+b_2'a_2+\cdots+b_n'a_n$$

ときめる．このとき，例えば，

$$a=(1-b_1)a_1+b_2'a_2+\cdots+b_n'a_n$$

から $a-a_1=-b_1a_1+b_2'a_2+\cdots+b_n'a_n$ で，$b_1, b_2', \cdots, b_n'$ はすべて A_1 に属するから $a-a_1 \in A_1$．同じように

$$a-a_i \in A_i, \quad a+A_i=a_i+A_i \quad (1 \leqq i \leqq n)$$

が成り立って，

$$f(a)=(a+A_1, a+A_2, \cdots, a+A_n)=(a_1+A_1, a_2+A_2, \cdots, a_n+A_n)$$

をうる．f は全射である．

f が環同型であること，f の核が $\bigcap_{i=1}^n A_i$ であることは明らか．

例 3　$m_1, m_2, \cdots, m_n$ は自然数で，$i \neq j$ ならば m_i, m_j は互いに素とする．このとき任意の整数 $b_1, b_2, \cdots, b_n$ に対して連立合同式

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \quad \cdots \\ x \equiv b_n \pmod{m_n} \end{cases}$$

は積 $m_1m_2\cdots m_n$ を法としてただ1個の解をもつことを示す．

まず，$i \neq j$ ならば $(m_i)+(m_j)=\boldsymbol{Z}$ であるから補題3.14から

$$f\colon \boldsymbol{Z} \to \prod_{i=1}^n \boldsymbol{Z}/(m_i), \quad a \to (a+(m_1), a+(m_2), \cdots, a+(m_n))$$

は全射環準同型で $\mathrm{Ker}\, f=\bigcap_{i=1}^n (m_i)$ である．特に $\prod_{i=1}^n \boldsymbol{Z}/(m_i)$ の元 $(b_1+(m_1), b_2+(m_2), \cdots, b_n+(m_n))$ に対してある $x \in \boldsymbol{Z}$ があって

$$(b_1+(m_1), b_2+(m_2), \cdots, b_n+(m_n))$$
$$=f(x)=(x+(m_1), x+(m_2), \cdots, x+(m_n)).$$

したがって, $b_1+(m_1)=x+(m_1)$, $b_2+(m_2)=x+(m_2)$, $\cdots$, $b_n+(m_n)=x+(m_n)$ で, これは

$$x-b_1\in(m_1), x-b_2\in(m_2), \cdots, x-b_n\in(m_n)$$

を意味する. x は上の連立合同式の解である.

もう1個 $y\in\boldsymbol{Z}$ が連立合同式の解ならば

$$f(y)=(b_1+(m_1), b_2+(m_2), \cdots, b_n+(m_n))=f(x)$$

となり, $x-y\in\mathrm{Ker}\,f=\bigcap_{i=1}^n(m_i)$. ここで $\bigcap_{i=1}^n(m_i)=(m_1m_2\cdots m_n)$ が成り立ち(この証明は演習問題とする), $x-y\in(m_1m_2\cdots m_n)$. 解は $m_1m_2\cdots m_n$ を法として一意的である.

環 R のイデアルを A とし, 剰余環 R/A をつくる. 環 R/A は R/A-加群であり $\pi: R\to R/A$ は環準同型であるから, R の元 a, R/A の元 $b+A$ に対して

$$a\cdot(b+A)=\pi(a)\cdot(b+A)=ab+A$$

ときめて R/A を R-加群とみれる(演習問題2).

補題3.14で $R/A_1, R/A_2, \cdots, R/A_n$ をこのように R-加群とみたとき, 直積 $\prod_{i=1}^n R/A_i$ は R-加群 $R/A_1, R/A_2, \cdots, R/A_n$ の外部直和とみれる. 写像

$$f: R\to\prod_{i=1}^n R/A_i, \quad a\to(a+A_1, a+A_2, \cdots, a+A_n)$$

は環準同型であったが, $b\in R$ に対して

$$f(ba)=(ba+A_1, ba+A_2, \cdots, ba+A_n)$$
$$=(b\cdot(a+A_1), b\cdot(a+A_2), \cdots, b\cdot(a+A_n))=b\cdot f(a)$$

は f が R から R-加群 $R/A_1, R/A_2, \cdots, R/A_n$ の外部直和への全射 R-準同型

$$f: R\to R/A_1\oplus R/A_2\oplus\cdots\oplus R/A_n$$

であることを示している. こうみても $\mathrm{Ker}\,f=\bigcap_{i=1}^n A_i$ であることはかわらない.

例 4 $\boldsymbol{Z}$-加群 $\boldsymbol{Z}/(6)$ は $\boldsymbol{Z}$-加群 $\boldsymbol{Z}/(2), \boldsymbol{Z}/(3)$ の外部直和と $\boldsymbol{Z}$-同型である. もっと一般に, a, b が互いに素な自然数ならば

$$\boldsymbol{Z}/(ab)\cong\boldsymbol{Z}/(a)\oplus\boldsymbol{Z}/(b)$$

が成り立つ(演習問題43参照).

例 5 単項イデアル整域が一意分解整域であることを用いれば, 定理3.13はもう少し詳しくのべられる.

Rを単項イデアル整域とする．0でも単元でもないRの元aは

$$a=p_1^{e_1}p_2^{e_2}\cdots p_n^{e_n}$$

（$p_1,p_2,\cdots,p_n$は相異なる素元，$e_1,e_2,\cdots,e_n$は自然数）

の形に分解される．ここで，例えば，$p_1\sim p_2$ならば$p_2=up_1$（uはRの単元）とかけるから$a=u^{e_2}p_1^{e_1+e_2}p_3^{e_3}\cdots p_n^{e_n}$とかきなおせる．互いに同伴なものがなくなるまでこの手続きをくりかえし，改めて

$$a=up_1^{e_1}p_2^{e_2}\cdots p_n^{e_n}\qquad（u\text{は}R\text{の単元，}p_1,p_2,\cdots,p_n\text{は互いに同伴でない素元，}e_1,e_2,\cdots,e_n\text{は自然数}）$$

の形に分解しておく．

まず，$i\neq j$ならば$R=Rp_i+Rp_j$であることを示す．$Rp_i+Rp_j=Ra$とおき，aがRの単元であることを示せばよい．$Rp_i\subseteqq Ra$でRp_iは極大イデアル（補題2.18）であるから$Rp_i=Ra$か$Ra=R$が成り立つ．aが単元でないならば$Rp_i=Ra$で，$p_i=ab$をみたすRの元bがある．補題2.18からbは単元であり$p_ib^{-1}=a$となる．全く同じようにして$p_jc^{-1}=a$をみたすRの単元cがある．このとき$p_ib^{-1}=p_jc^{-1}$となり，p_i,p_jは互いに同伴となって矛盾である．

演習問題2の24から$R=Rp_i^{e_i}+Rp_j^{e_j}$が成り立つが，

$$Ra=Rp_1^{e_1}p_2^{e_2}\cdots p_n^{e_n}=Rp_1^{e_1}\cdot Rp_2^{e_2}\cdot\cdots\cdot Rp_n^{e_n}=\bigcap_{i=1}^{n}Rp_i^{e_i}$$

である（演習問題43, 44参照）から，補題3.14を用いてR-加群とみて

$$R/Ra\cong R/Rp_1^{e_1}\oplus R/Rp_2^{e_2}\oplus\cdots\oplus R/Rp_n^{e_n}.$$

一般に，$\{0\}$でないR-加群Mが**直既約**とは，Mの部分加群M_1,M_2があって

$$M=M_1\oplus M_2\ \Rightarrow\ M_1=\{0\}\ \text{または}\ M_2=\{0\}$$

であるときめる．

例えば，単純R-加群は直既約であり，Rが整域ならば，RはR-加群とみて直既約である．実際，$R=A_1\oplus A_2$と2つの$\{0\}$でないイデアルA_1,A_2の内部直和に分解されたとする．A_1,A_2はそれぞれ0でない元a_1,a_2を含み，$a_1a_2\in A_1\cap A_2=\{0\}$であるが，これは$a_1a_2\neq 0$に矛盾する．

例 6　例5の分解にあらわれるR/Rp^eの形の巡回加群は直既約である．

R/Rp^eの部分加群はRp^m/Rp^e $(0\leqq m\leqq e)$の形をしている（3.1節例11）．もしR/Rp^eが直既約でないならば

$$R/Rp^e=Rp^m/Rp^e\oplus Rp^n/Rp^e\qquad(0<m,n<e)$$

の形に分解できる．したがって，

$$R=Rp^m+Rp^n=Rp^l \qquad (l=\min\{m,n\})$$

となり，$l>0$ であるから p は単元となって矛盾である．

R は単項イデアル整域，$a\in R$ とする．例5の証明から R/Ra が直既約ならば，a の素元分解はただ1個の素元 p によって $a=p^e$ の形をしている．したがって，

$$R/Ra \text{ が直既約} \Leftrightarrow a \text{ の素元分解が } p^e \text{ の形}$$

が成り立つ．このことから例5の分解

$$R/Ra\cong R/Rp_1^{e_1}\oplus R/Rp_2^{e_2}\oplus\cdots\oplus R/Rp_n^{e_n}$$

は，a の互いに同伴でない素元への分解 $a=up_1^{e_1}p_2^{e_2}\cdots p_n^{e_n}$ と R/Ra の直既約加群への直和分解とが対応していることを意味する．

3.6 アーベル群の基本定理 (2)

この節では定理3.13の分解の一意性を示す．

定理 3.15 R は単項イデアル整域，M は有限生成加群とする．M が

$$M\cong(\oplus_{i=1}^n R/Ra_i)\oplus R^s\cong(\oplus_{i=1}^m R/Rb_i)\oplus R^t$$

$$(R\neq Ra_1\supseteqq Ra_2\supseteqq\cdots\supseteqq Ra_n\neq\{0\},\ R\neq Rb_1\supseteqq Rb_2\supseteqq\cdots\supseteqq Rb_m\neq\{0\})$$

と直和に分解されるならば，

$$n=m,\quad Ra_i=Rb_i\quad(1\leqq i\leqq n),\quad s=t$$

が成り立つ．

定理3.15において M によって一意的にきまる R のイデアル

$$Ra_1, Ra_2, \cdots, Ra_n$$

を M の**不変因子**とよぶ．また，自然数 s も M によって一意的にきまる．これを M の**階数**とよぶ．

定理3.15の証明のために，トーション加群の説明からはじめる．

R を整域とし，M を R-加群とする．M の元 x が R 上1次独立でないとき，すなわち，$\mathrm{Ann}_R\, x\neq\{0\}$ のとき，x を M の**トーション** (torsion) **元**とよぶ．M の零元は明らかにトーション元である．

M のトーション元の全体を $t(M)$ とかく．

$$t(M)=\{x\in M\mid \mathrm{Ann}_R\, x\neq\{0\}\}.$$

R が整域であるから $t(M)$ は M の部分加群をつくる．これを M の**トーション部分加群**とよぶ．

M の $t(M)$ による剰余加群 $M/t(M)$ は零元以外にトーション元をもたない．実際，$M/t(M)$ の元 $x+t(M)$ がある $a\in R$，$a\neq 0$ に対して $a\cdot(x+t(M))=0+t(M)$ ならば，$ax\in t(M)$ であるから，ある $b\in R$，$b\neq 0$ があって $0=b\cdot(ax)=(ba)x$．$ba\neq 0$ から $x\in t(M)$ で $x+t(M)=0+t(M)$ となる．

特に，$t(M)=M$ である R-加群 M をトーション R-加群または単に**トーション加群**とよぶ．$t(M)=\{0\}$ である M を**トーション・フリー加群**とよぶ．R-加群 M に対して $M/t(M)$ はトーション・フリー加群である．

例 1　アーベル群 G を $\boldsymbol{Z}$-加群とみるとき，G の元 x がトーション元とは x の位数が有限であることにほかならない．

例 2　n を自然数として $\boldsymbol{Z}/(n)$ を $\boldsymbol{Z}$-加群とみるとき，どの元も n 倍すれば零元となるからすべてトーション元である．$\boldsymbol{Z}/(n)$ はトーション加群である．

例 3　$\boldsymbol{R}$ の上のベクトル空間 M では，トーション元は零元しかない．M はトーション・フリー加群である．

例 4　整域 R を R-加群とみるときもトーション元は零元しかない．R はトーション・フリー加群である．

例 5　$\boldsymbol{Q}$ は $\boldsymbol{Z}$-加群とみてトーション・フリー加群である．

例 2, 4 を一般的にのべると

例 6　R を整域，$M=Rx$ を $\{0\}$ でない巡回 R-加群とすれば，

(1)　$t(M)=M \Leftrightarrow \mathrm{Ann}_R\, x\neq\{0\}$.

(2)　$t(M)=\{0\} \Leftrightarrow \mathrm{Ann}_R\, x=\{0\}$.

この証明は演習問題とする．

M, N が R-加群で $f\colon M\to N$ が R-準同型ならば，

$$f(t(M))\subseteq t(N)$$

が成り立ち，特に，f が R-同型であるときは

$$f(t(M))=t(N),\quad t(M)\cong t(N).$$

また，R-加群 M が部分加群 M_1, M_2 の内部直和であるときは

$$t(M)=t(M_1)\oplus t(M_2)$$

が成り立つ．これらの証明も演習問題とする．

定理 3.15 の証明のために補題を 2 つ用意する．

補題 3.16　R は単項イデアル整域，p は R の素元，e は自然数とする．このとき $f, g\in\mathrm{End}({}_RR/Rp^e)$, $f+g=1$ ならば，f, g のいずれかは R-同型である．

証明　R/Rp^e の部分加群は Rp^k/Rp^e $(0 \leqq k \leqq e)$ でつくされる．特に，Rp^{e-1}/Rp^e は R/Rp^e の $\{0\}$ でない部分加群の中で最小である (3.1 節例 11).

もし $\mathrm{Ker}\, f$, $\mathrm{Ker}\, g$ が共に $\{0\}$ でないならば，$Rp^{e-1}/Rp^e \subseteqq (\mathrm{Ker}\, f) \cap (\mathrm{Ker}\, g)$ で $\{0\} \neq Rp^{e-1}/Rp^e = (f+g)(Rp^{e-1}/Rp^e) \subseteqq f(Rp^{e-1}/Rp^e) + g(Rp^{e-1}/Rp^e) = \{0\}$ で矛盾である．したがって，$\mathrm{Ker}\, f$, $\mathrm{Ker}\, g$ のいずれかは $\{0\}$ である．

$\mathrm{Ker}\, f = \{0\}$ のときは，ある k $(0 \leqq k \leqq e)$ があって

$$R/Rp^e \cong f(R/Rp^e) = Rp^k/Rp^e \cong R/Rp^{e-k}.$$

$Rp^e = \mathrm{Ann}_R(R/Rp^e) = \mathrm{Ann}_R(R/Rp^{e-k}) = Rp^{e-k}$. したがって，$R$ の単元 u があって $p^e = up^{e-k}$. 素元分解の一意性から $e = e-k$, $k = 0$. このことは $f(R/Rp^e) = R/Rp^e$ を意味し，f は全射である．$\mathrm{Ker}\, g = \{0\}$ のときも同様である．

補題 3.17　R は単項イデアル整域，T_1, T_2 は R-同型な素数べき位数の巡回加群とする．このとき，R-加群 M_1, M_2 に対して

$$M_1 \oplus T_1 \cong M_2 \oplus T_2$$

ならば，M_1, M_2 は R-同型である．

証明　$f: M_1 \oplus T_1 \to M_2 \oplus T_2$ を与えられた R-同型とすれば，

$$M_2 \oplus T_2 = f(M_1 \oplus T_1) = f(M_1) \oplus f(T_1).$$

ここで $f(T_1) \cong T_1 \cong T_2$ であり，$f(M_1) \cong M_1$ である．したがって，$f(M_1) \cong M_2$ が証明できれば，$M_1 \cong M_2$ をうる．このことは，M_1, T_1 を $f(M_1), f(T_1)$ でおきかえて，$M_1 \oplus T_1 = M_2 \oplus T_2$ ならば $M_1 \cong M_2$ を証明すればよいことを示している．

$M = M_1 \oplus T_1 = M_2 \oplus T_2$ とおき，この分解に関する射影，入射を

$$M_1 \underset{p_1}{\overset{\nu_1}{\rightleftarrows}} M \underset{p_2}{\overset{\nu_2}{\leftrightarrows}} T_1, \quad M_2 \underset{p_1'}{\overset{\nu_1'}{\rightleftarrows}} M \underset{p_2'}{\overset{\nu_2'}{\leftrightarrows}} T_2$$

とおく．$\nu_1'p_1' + \nu_2'p_2' = 1_M$ から

$$p_2(\nu_1'p_1' + \nu_2'p_2')\nu_2 = p_2 1_M \nu_2 = 1_{T_1}.$$

$p_2\nu_1'p_1'\nu_2$, $p_2\nu_2'p_2'\nu_2$ は共に $\mathrm{End}({}_R T_1)$ に属するから，$p_2\nu_1'p_1'\nu_2$ か $p_2\nu_2'p_2'\nu_2$ のいずれかが R-同型である (補題 3.16)．$p_2\nu_1'p_1'\nu_2$ が R-同型とする．この逆写像を f_1 とかけば $(f_1 p_2) \cdot (\nu_1'p_1'\nu_2) = 1_{T_1}$. したがって，

$$M = (\mathrm{Ker}\, f_1 p_2) \oplus \nu_1'p_1'\nu_2(T_1)$$

(補題 3.5)．$\mathrm{Ker}\, f_1 p_2 = \mathrm{Ker}\, p_2 = M_1$ であるから

$$M = M_1 \oplus \nu_1'p_1'\nu_2(T_1). \qquad \cdots\cdots①$$

$\nu_1'p_1'\nu_2(T_1) \subseteqq M_2$ から

$$M_2 = (M_1 \cap M_2) \oplus \nu_1'p_1'\nu_2(T_1) \qquad \cdots\cdots②$$

(演習問題 29). ① と $M=M_1\oplus T_1$ からは

$$\nu_1'p_1'\nu_2(T_1)\cong M/M_1\cong T_1\cong T_2. \qquad \cdots\cdots③$$

② と $M=M_2\oplus T_2$ からは

$$M=M_2\oplus T_2=(M_1\cap M_2)\oplus\nu_1'p_1'\nu_2(T_1)\oplus T_2. \qquad \cdots\cdots④$$

①, ④, ③, ② の順に上の関係を用いて

$$M_1\cong M/\nu_1'p_1'\nu_2(T_1)\cong(M_1\cap M_2)\oplus T_2\cong(M_1\cap M_2)\oplus\nu_1'p_1'\nu_2(T_1)=M_2$$

をうる.

$p_2\nu_2'p_2'\nu_2$ が R-同型のときは, その逆写像を f_2 とかくと

$$M=(\mathrm{Ker}\, f_2p_2)\oplus\nu_2'p_2'\nu_2(T_1)=M_1\oplus\nu_2'p_2'\nu_2(T_1). \qquad \cdots\cdots⑤$$

$\nu_2'p_2'\nu_2(T_1)\subseteqq T_2$ から

$$T_2=(M_1\cap T_2)\oplus\nu_2'p_2'\nu_2(T_1).$$

しかし, T_2 は直既約であり (3.5 節例 6), $\nu_2'p_2'\nu_2(T_1)\neq\{0\}$ であるから $T_2=\nu_2'p_2'\nu_2(T_1)$. ⑤ から $M=M_1\oplus T_2$.

したがって, $M=M_2\oplus T_2$ とあわせて

$$M_2\cong M/T_2\cong M_1.$$

定理 3.15 の**証明**.

$$M\cong(\oplus_{i=1}^{n}R/Ra_i)\oplus R^s\cong(\oplus_{i=1}^{m}(R/Rb_i))\oplus R^t$$
$$(R\neq Ra_1\supseteqq Ra_2\supseteqq\cdots\supseteqq Ra_n\neq 0,\ R\neq Rb_1\supseteqq Rb_2\supseteqq\cdots\supseteqq Rb_m\neq 0)$$

とする. R-同型 $(\oplus R/Ra_i)\oplus R^s\to(\oplus R/Rb_i)\oplus R^t$ を f とかく.

まず, トーション部分加群を考えると

$$f(t((\oplus R/Ra_i)\oplus R^s))=t((\oplus R/Rb_i)\oplus R^t).$$

この左辺は $f(\oplus R/Ra_i)$, 右辺は $\oplus R/Rb_i$ に等しい. $f(\oplus R/Ra_i)\oplus f(R^s)=f((\oplus R/Ra_i)\oplus R^s)=(\oplus R/Rb_i)\oplus R^t$ であるから

$$f(R^s)\cong R^t.$$

したがって, $s=t$ であることが分かる.

次に, $f(\oplus_{i=1}^{n}R/Ra_i)=\oplus_{i=1}^{m}R/Rb_i$ から $n=m$, $Ra_i=Rb_i$ $(1\leqq i\leqq n)$ を, $n\geqq m$ として n に関する帰納法で示す.

$n=1$ のとき, $m=0$ ではありえないから $m=1$ で, このときは

$$Ra_1=\mathrm{Ann}_R\, R/Ra_1=\mathrm{Ann}_R\, R/Rb_1=Rb_1$$

である (3.2 節例 5).

$n>1$ とし, $\oplus_{i=1}^{n-1}R/Ra_i\cong\oplus_{i=1}^{m-1}R/Rb_i$ ならば, $n-1=m-1$ で $Ra_i=Rb_i$ (1≦

$i\leqq n-1$) であるものと仮定する．$a_n\cdot(\oplus_{i=1}^{n}R/Ra_i)=0$ から

$$a_n\cdot(\oplus_{i=1}^{m}R/Rb_i)=0,\ \text{特に}\ a_n\cdot R/Rb_m=0.$$

したがって，$a_n\in Rb_m$, $Ra_n\subseteqq Rb_m$ をうる．同じようにして $Rb_m\subseteqq Ra_n$ で $Ra_n=Rb_m$ となる．

a_n は 0 でも単元でもないから

$$a_n=up_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$$

（u は R の単元，$p_1, p_2, \cdots, p_k$ は互いに同伴でない R の素元，$e_1, e_2, \cdots, e_k$ は自然数）

(3.5 節例 5）と分解できる．b_m も同じように分解する．

$$b_m=vq_1^{f_1}q_2^{f_2}\cdots q_h^{f_h}.$$

このとき，

$$k=h,\ \ p_i\sim q_i,\ \ e_i=f_i \qquad (1\leqq i\leqq n)$$

であることを示す．

$Ra_n=Rb_m$ からある R の単元 w があって

$$up_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}=a_n=wb_m=wvq_1^{f_1}q_2^{f_2}\cdots q_h^{f_h}.$$

up_1 は素元である（演習問題 2 の 51）から u を，例えば，$(up_1)\cdot p_1^{e_1-1}p_2^{e_2}\cdots p_k^{e_k}$ のように分解の中にくりこむ．wv も同じようにくりこむ．このとき，素元分解の一意性から

$$e_1+e_2+\cdots+e_k=f_1+f_2+\cdots+f_h,$$

各 p_i は適当な q_j と互いに同伴

とできる．簡単に $p_1\sim q_1$ とする．$p_1^{e_1}\sim q_1^{e_1}$ でもある．もし $e_1<f_1$ ならば

$$up_2^{e_2}\cdots p_k^{e_k}=wvq_1^{f_1-e_1}q_2^{f_2}\cdots q_h^{f_h}.$$

ある i に対して $q_1\sim p_i$ であるが，$p_1\sim q_1\sim p_i$ で矛盾を生ずる．したがって，$e_1=f_1$ である．同じようにして

$$k=h,\quad p_2\sim q_2, \cdots, p_k\sim q_k,\quad e_2=f_2, \cdots, e_k=f_k$$

となる．

3.5 節例 4 から

$$R/Ra_n=R/Rb_m\cong R/Rp_1^{e_1}\oplus R/Rp_2^{e_2}\oplus\cdots\oplus R/Rp_k^{e_k}.$$

したがって，

$$(\oplus_{i=1}^{n-1}R/Ra_i)\oplus R/Rp_1^{e_1}\oplus R/Rp_2^{e_2}\oplus\cdots\oplus R/Rp_k^{e_k}$$
$$\cong(\oplus_{i=1}^{m-1}R/Rb_i)\oplus R/Rp_1^{e_1}\oplus R/Rp_2^{e_2}\oplus\cdots\oplus R/Rp_k^{e_k}$$

で，補題 3.17 をくりかえし用いれば

$$\oplus_{i=1}^{n-1}R/Ra_i\cong\oplus_{i-1}^{m-1}R/Rb_i$$

をうる．ここに帰納法の仮定を適用すればよい．

Gを有限生成アーベル群とする．Gの演算を加法でかき，Gを$\boldsymbol{Z}$-加群とみる．$\boldsymbol{Z}$は単項イデアル整域であるからGにこの節と前節の結果を適用することができる．まず，定理3.13, 3.15を用いて

定理 3.18　有限生成アーベル群Gは

$$G \cong (\oplus_{i=1}^{n} \boldsymbol{Z}/(a_i)) \oplus \boldsymbol{Z}^s$$

の形に分解される．ここで$a_1, a_2, \cdots, a_n$は自然数（>1）で

$$a_1 | a_2 | \cdots | a_n$$

をみたす．その上，この$a_1, a_2, \cdots, a_n$とsはGによって一意的にきまる．

定理3.15によれば，一意的にきまるのはa_iではなく(a_i)であるが，a_iを自然数としているので，(a_i)がきまれば(a_i)に含まれる最小の自然数としてa_iがきまる．この意味で$a_1, a_2, \cdots, a_n$をGの**不変因子**とよぶ．また，$\oplus_{i=1}^{n} \boldsymbol{Z}/(a_i)$は$G$のトーション部分加群$t(G)$と同型であり，$\boldsymbol{Z}^s$は階数$s$の自由加群であることを注意しておこう．

3.5節例5から次の定理がえられる．

定理 3.19　有限生成アーベル群Gは

$$G \cong (\oplus_{i=1}^{n} \boldsymbol{Z}/({p_i}^{e_i})) \oplus \boldsymbol{Z}^s$$

の形に分解される．ここで$p_1, p_2, \cdots, p_n$は素数で，${p_1}^{e_1}, {p_2}^{e_2}, \cdots, {p_n}^{e_n}$は順序を除いて$s$と共に$G$によって一意的にきまる．

定理3.19の直和分解にあらわれる素数べき${p_i}^{e_i}$をGの**単因子**とよぶ．ここでp_iがすべて異なるとはかぎらない．同じ素数べき${p_i}^{e_i}$が上の直和分解にあらわれる回数を${p_i}^{e_i}$のGにおける**重複度**とよぶ．

定理3.18, 3.19の2つの定理をあわせて，**アーベル群の基本定理**という．

Gが有限生成でなく，有限アーベル群であるときは，Gはトーション加群であって$G \cong \oplus_{i=1}^{n} \boldsymbol{Z}/({p_i}^{e_i})$となる．このとき，$G$の各単因子を重複度に等しい個数だけ並べて$G$をあらわすことがある．例えば，

$$(2, 2, 2^3, 5^2, 5^2)$$

とかけば，Gが

$$\boldsymbol{Z}/(2) \oplus \boldsymbol{Z}/(2) \oplus \boldsymbol{Z}/(2^3) \oplus \boldsymbol{Z}/(5^2) \oplus \boldsymbol{Z}/(5^2)$$

に同型なアーベル群であることを意味する．明らかに，このとき，Gの位数は

$$|G|=2\cdot 2\cdot 2^3\cdot 5^2\cdot 5^2$$

である.

例 7　位数 12 のアーベル群をすべて求めてみよう.

位数の 12 をいくつかの素数の積にあらわす方法が何通りあるかを考える. $12=2^2\cdot 3$ であるから，あらわし方は

$$2^2\cdot 3 \quad と \quad 2\cdot 2\cdot 3$$

の二通りがあり，それにしたがって

$$(2^2, 3)\ 型のアーベル群と\ (2, 2, 3)\ 型のアーベル群,$$

$$\boldsymbol{Z}/(2^2)\oplus\boldsymbol{Z}/(3) \quad と \quad \boldsymbol{Z}/(2)\oplus\boldsymbol{Z}/(2)\oplus\boldsymbol{Z}/(3)$$

に同型なものの 2 つがある.

3.5 節の例 4 を用いると $\boldsymbol{Z}/(2^2)\oplus\boldsymbol{Z}/(3)\cong\boldsymbol{Z}/(12)$ であるから，これは巡回群である．実際，$(1+(2^2), 1+(3))$ が位数 12 で生成元になっている.

例 8　有限アーベル群 G には位数最大の元が存在し，この位数を n とかけば，G の任意の元の位数は n の約数である.

G を

$$G=G_1\oplus G_2\oplus\cdots\oplus G_n \qquad (G_i\ は位数\ a_i\ (\neq 0)\ の巡回部分加群)$$

$$a_1 | a_2 | \cdots | a_n$$

とかく．このとき，$a_{i+1}=a_i b_{i+1}$ $(1\leqq i\leqq n-1)$ とかけば

$$a_n=a_i b_{i+1} b_{i+2}\cdots b_n \qquad (1\leqq i\leqq n-1)$$

とあらわされる．G_i の生成元を x_i とおけば，G の任意の元 x は

$$x=m_1x_1+m_2x_2+\cdots+m_nx_n \qquad (m_i\in\boldsymbol{Z})$$

とあらわされ，

$$a_nx=m_1a_1b_2\cdots b_nx_1+m_2a_2b_3\cdots b_nx_2+\cdots+m_na_nx_n=0$$

であるから，x の位数は a_n の約数であり（1.4 節例 7），したがって，x_n が G の位数最大の元である.

演習問題 3

1.　R を環，M を R-加群とする．$a\in R$, $x\in M$ に対して

$$(-a)x=-(ax)=a(-x)$$

が成り立つことを示せ.

2.　R, S が環で $f\colon R\to S$ が環準同型とする．このとき，S-加群 ${}_SM$ を

$$\varphi\colon R\times M\to M, \quad (a, x)\to f(a)x$$

ときめると，R-加群にできることを示せ．

3.　R-加群Mの空でない部分集合Sに対して，Sを含むMの部分加群すべての共通部分はまたMの部分加群であることを示せ．

4.　R-加群Mの有限部分集合$S=\{x_1, x_2, \cdots, x_n\}$ に対して

$$R\cdot S=Rx_1+Rx_2+\cdots+Rx_n$$

を示せ．

5.　MをR-加群，$M_1, M_2, \cdots, M_n$をMの部分加群，$S=M_1\cup M_2\cup\cdots\cup M_n$とすれば，

$$R\cdot S=M_1+M_2+\cdots+M_n$$

であることを示せ．

6.　R-加群Mの部分集合Sに対して

$$\mathrm{Ann}_R\, S=\{a\in R \mid \text{任意の } s\in S \text{ に対して } as=0\}$$

とおく．次のことを示せ．

(1)　$\mathrm{Ann}_R\, S$はRの左イデアルである．

(2)　Rが可換で$M=Rx$が巡回加群ならば$\mathrm{Ann}_R\, M=\mathrm{Ann}_R\, x$．

7.　前問で$S=M$とおいた$\mathrm{Ann}_R M$はRのイデアルであり，剰余環$R/\mathrm{Ann}_R M$をつくれば，Mは$R/\mathrm{Ann}_R\, M$の上の加群でもあることを示せ．

8.　MをR-加群，M'を部分加群とする．$M', M/M'$が共に有限生成加群ならば，Mも有限生成加群であることを示せ．

9.　素数pに対して$M=\left\{\dfrac{a}{p^n}\in Q \mid a\in \boldsymbol{Z}, n \text{は自然数}\right\}$とおく．次のことを示せ．

(1)　Mは$\boldsymbol{Z}$-加群$\boldsymbol{Q}$の部分加群で$\boldsymbol{Z}$を含む．

(2)　剰余加群$M/\boldsymbol{Z}$を$\boldsymbol{Z}_{p^\infty}$とかく．$H$を$\boldsymbol{Z}_{p^\infty}$の自明でない部分加群とし，$\dfrac{a}{p^m}+\boldsymbol{Z}\in H, (a, p^m)=1$ならば，任意の$b\in\boldsymbol{Z}$，任意の自然数$n\leqq m$に対して$\dfrac{b}{p^n}+\boldsymbol{Z}\in H$である．

(3)　ある自然数nがあって$\dfrac{1}{p^n}+\boldsymbol{Z}\notin H$であるが，このような$n$の最小数は1より大きく，これを$s+1$とかけば

$$H=\left\{\frac{a}{p^m}+\boldsymbol{Z} \mid m\leqq s, a\in\boldsymbol{Z}\right\}.$$

(4)　Hは$\dfrac{1}{p^s}+\boldsymbol{Z}$から生成された巡回加群である．

(5)　$\boldsymbol{Z}_{p^\infty}$の自明でない2つの部分加群の間に大小関係がある．

(6) $\boldsymbol{Z}_{p^\infty}$ は極大部分加群をもたない．

10. M, N が R–加群，$f: M \to N$ が R–準同型ならば，M の部分加群 M', N の部分加群 N' に対して，$f(M')$ は N の，$f^{-1}(N')$ は M の部分加群であることを示せ．

11. アーベル群を $\boldsymbol{Z}$–加群とみたとき，加法群としての準同型が $\boldsymbol{Z}$–準同型であることを示せ．

12. 環 R を R–加群 ${}_RR$ とみたとき，${}_RR$ の R–準同型と R の環準同型とは同じものであるとはかぎらないことを次の例で確かめよ．

(1) $R=\boldsymbol{Z}$ で $f: \boldsymbol{Z} \to \boldsymbol{Z}$, $a \to 2a$ は $\boldsymbol{Z}$–準同型ではあるが，環準同型ではない．

(2) $R=\boldsymbol{C}$ で $f: \boldsymbol{C} \to \boldsymbol{C}$, $\alpha \to \bar{\alpha}$ は環準同型ではあるが，$\boldsymbol{C}$–準同型ではない．ここで $\bar{\alpha}$ は $\alpha \in \boldsymbol{C}$ の共役複素数をあらわす．

13. R を整域，$a \in R$, $a \neq 0$ とする．このとき，次のことを示せ．

(1) R–加群として $R \cong Ra$ である．

(2) Ra が R の部分環 $\Leftrightarrow$ a が R の単元

(3) (2)の同値条件が成り立つとき，R と Ra は環同型である．

14. R が可換環で A, B が R のイデアルならば

$$R\text{–加群として } R/A \cong R/B \Leftrightarrow A=B$$

を示せ．

15. M, N は R–加群，$f: M \to N$ は R–準同型とする．このとき $\mathrm{Ker}\, f$ に含まれる M の部分加群 K に対して，図 3.7 の図型が可換となる R–準同型 $g: M/K \to N$ がただ 1 つ存在することを示せ．

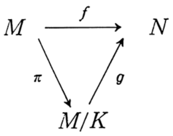


図 3.7

16. R–加群 M, 部分加群 K, H に対して

$$(K+H)/H \cong K/(K \cap H) \quad (R\text{–同型})$$

を示せ（演習問題 1 の 30 参照）．

17. M が R–加群，K, H は部分加群で $K \subseteq H$ ならば

$$(M/K)/(H/K) \cong M/H \quad (R\text{–同型})$$

を示せ（定理 1.20 参照）．

18.　R-加群 M, N に対して M から N への R-準同型の全体 $\mathrm{Hom}_R(M, N)$ は加法群をつくることを示せ．特に，M から M への R-準同型の全体 $\mathrm{Hom}_R(M, M)$ を $\mathrm{End}({}_RM)$ とかく．$\mathrm{End}({}_RM)$ は環をつくることを示せ（2.1 節例 4 参照）．

19.　M が単純 R-加群ならば，$\mathrm{End}({}_RM)$ は斜体であることを示せ（これを**シュアーの補題**という）．

20.　M を R-加群，$\mathrm{End}({}_RM)$ を S とおいて，次のことを示せ．

(1)　写像 $S\times M\to M$ を $(f, x)\to f(x)$ ときめると，M は S-加群である．

(2)　$a\in R$ ならば f_a: $M\to M$，$x\to ax$ は S-準同型である．

21.　L, M, N を R-加群，f: $L\to M$，g: $M\to N$ を R-準同型とする．R-加群と R-準同型の列

$$L \xrightarrow{f} M \xrightarrow{g} N$$

が M で**完全**とは $f(L)=\mathrm{Ker}\, g$ が成り立つことときめる．

R-加群と R-準同型の可換図型（図 3.8）で上の列は M で，下の列は M' で完全であるとする．このとき，次のことを示せ．

$$\begin{array}{ccccc}
L & \xrightarrow{f} & M & \xrightarrow{g} & N \\
{\scriptstyle\alpha}\downarrow & \circlearrowright & \downarrow{\scriptstyle\beta} & \circlearrowright & \downarrow{\scriptstyle\gamma} \\
L' & \xrightarrow[f']{} & M' & \xrightarrow[g']{} & N'
\end{array}$$

図 3.8

(1)　α, γ, f' が単射 $\Rightarrow$ β が単射．

(2)　α, γ, g が全射 $\Rightarrow$ β が全射．

(3)　β が単射，α, g が全射 $\Rightarrow$ γ が単射．

(4)　β が全射，f', γ が単射 $\Rightarrow$ α が全射．

22.　$$\cdots \to \boldsymbol{Z}/(4) \to \boldsymbol{Z}/(4) \to \boldsymbol{Z}/(4) \to \cdots$$

はすべての $\boldsymbol{Z}/(4)$ で完全な $\boldsymbol{Z}$-加群と $\boldsymbol{Z}$-準同型の列であることを示せ．

23.　$M=\{0, x, y, z\}$ を位数 4 の $\boldsymbol{Z}$-加群で巡回加群ではないとする．このとき，次のことを示せ．

(1)　$x+y=z$，$y+z=x$，$z+x=y$．

(2)　$M=\boldsymbol{Z}x\oplus\boldsymbol{Z}y=\boldsymbol{Z}y\oplus\boldsymbol{Z}z=\boldsymbol{Z}z\oplus\boldsymbol{Z}x$．

24.　R-加群 M が部分加群 $M_1, M_2, \cdots, M_n$ の内部直和

$\Leftrightarrow$ (1)　$M=M_1+M_2+\cdots+M_n$,

(2)　$(M_1+M_2+\cdots+M_{i-1})\cap M_i=\{0\}$　　$(2\leqq i\leqq n)$

であることを示せ．

25.　$M=M_1\oplus M_2\oplus\cdots\oplus M_n$ を R-加群Mの部分加群の内部直和，$p_i\colon M\to M_i$ を i-射影とする．このとき，次のことを示せ．

(1)　$\sum_{i=1}^n p_i=1_M$.　　(2)　$p_i{}^2=p_i$.　　(3)　$p_ip_j=0$　$(i\neq j)$.

(4)　逆に，Mが R-加群，$p_1, p_2, \cdots, p_n$ がMからMへの R-準同型で，(1), (2), (3)をみたすとき，$M_i=p_i(M)$ はMの部分加群で

$$M=M_1\oplus M_2\oplus\cdots\oplus M_n$$

であり，この直和分解によるi-射影が p_i と一致することを示せ．

26.　$M_1, M_2, \cdots, M_n$ を R-加群，$M_1\oplus M_2\oplus\cdots\oplus M_n$ をその外部直和とする．このとき，i-射影 p_i，i-入射 ν_i に対して次のことを示せ．

(1)　$\sum_{i=1}^n \nu_ip_i=1_M$.　　(2)　$p_i\nu_i=1_{M_i}$.　　(3)　$p_i\nu_j=0$　$(i\neq j)$.

27.　Rは可換環，Mは R-加群，$a\in R$ とする．このとき，次のことを示せ．

(1)　$f\colon M\to M$，$x\to ax$ はMの R-自己準同型である．

(2)　f の核を $\mathrm{Ann}_M\, a$，f の像を aM とかく．もしMが M_1, M_2 の内部直和ならば，$f|_{M_i}$ の核 $\mathrm{Ann}_{M_i}\, a$，$f|_{M_i}$ の像 aM_i に対して

$$aM=aM_1\oplus aM_2,\quad \mathrm{Ann}_M\, a=(\mathrm{Ann}_{M_1}\, a)\oplus(\mathrm{Ann}_{M_2}\, a).$$

28.　Mは R-加群で部分加群 M_1, M_2 の内部直和とする．R-自己準同型 $f\colon M\to M$ が $f(M_1)\subseteqq M_1$，$f(M_2)\subseteqq M_2$ をみたせば

$$f(M)=f(M_1)\oplus f(M_2),\quad \mathrm{Ker}\, f=(\mathrm{Ker}\, f|_{M_1})\oplus(\mathrm{Ker}\, f|_{M_2})$$

であることを示せ．

29.　Mは R-加群で部分加群 M_1, M_2 の内部直和とする．M'が部分加群で $M_1\subseteqq M'$ ならば

$$M'=M_1\oplus(M_2\cap M')$$

であることを示せ．

30.　環Rの上の $n\times n$ 行列の全体 $(R)_n$ に対して次のことを示せ．

(1)　$R\ni a, (R)_n\ni(a_{ij})$ に対して $a\cdot(a_{ij})=(aa_{ij})$ ときめて $(R)_n$ は R-加群をつくる．

(2)　$(R)_n\cong R^{n^2}$ である．

31.　$\boldsymbol{R}$ の上の三角行列環を $R=\begin{pmatrix}\boldsymbol{R} & \boldsymbol{R}\\ 0 & \boldsymbol{R}\end{pmatrix}$ とかく．$\begin{pmatrix}\boldsymbol{R} & 0\\ 0 & 0\end{pmatrix}, \begin{pmatrix}0 & \boldsymbol{R}\\ 0 & \boldsymbol{R}\end{pmatrix}$ は共にRを R-加群とみたときの部分加群であり

$$R=\begin{pmatrix}\boldsymbol{R} & 0\\ 0 & 0\end{pmatrix}\oplus\begin{pmatrix}0 & \boldsymbol{R}\\ 0 & \boldsymbol{R}\end{pmatrix}$$

であることを示せ．

32. MはR-加群で部分加群M', M''の内部直和とする．もしM'がM'の部分加群$M_1', M_2', \cdots, M_n'$の内部直和，M''がM''の部分加群$M_1'', M_2'', \cdots, M_m''$の内部直和ならば，$M$は$M_1', M_2', \cdots, M_n', M_1'', M_2'', \cdots, M_m''$の内部直和であることを示せ．

33. M_1, M_2, M_1', M_2'はR-加群で$M_1 \cong M_1'$, $M_2 \cong M_2'$ならば，M_1とM_2の外部直和はM_1'とM_2'の外部直和とR-同型であることを示せ．

34. MをR-加群, Nを部分加群とし, $\nu: N \to M$を包含写像, $\pi: M \to M/N$を標準的R-準同型とする．このとき，

$$R\text{-準同型 } f: M/N \to M \text{ があって } \pi f = 1_{M/N}$$
$$\Leftrightarrow R\text{-準同型 } p: M \to N \text{ があって } p\nu = 1_N$$

であることを示せ．

35. MをR-加群，$x_1, x_2, \cdots, x_n \in M$とする．このとき，次のことを示せ．

$x_1, x_2, \cdots, x_n$がR上1次独立

$\Leftrightarrow$ $\{x_1, x_2, \cdots, x_n\}$から生成された$M$の部分加群が$\oplus_{i=1}^n Rx_i$に等しい．

36. 有限加法群は$\boldsymbol{Z}$-加群とみて自由加群でないことを示せ．

37. $\boldsymbol{Q}$は$\boldsymbol{Z}$-加群とみて自由加群ではないことを示せ．

38. Rを斜体，MをR-加群（$\neq \{0\}$），$x_1, x_2, \cdots, x_n$をMの基底とする．xはMの元で$x = a_1x_1 + a_2x_2 + \cdots + a_nx_n$ ($a_i \in R, a_1 \neq 0$) とする．このとき，$x, x_2, \cdots, x_n$もMの基底であることを示せ．

39. MがR-加群，$X = \{x_1, x_2, \cdots, x_n\}$を$M$の部分集合とする．このとき，

Mが$x_1, x_2, \cdots, x_n$を基底とする自由加群

$\Leftrightarrow$ (1)　$M = Rx_1 + Rx_2 + \cdots + Rx_n$,

(2)　任意のR-加群NとXからNへの任意の写像fに対して

R-準同型$g: M \to N$があって$g|_X = f$

であることを示せ．

40. Mは自由R-加群，L, NはR-加群で$g: L \to N$が全射R-準同型ならば，任意のR-準同型$f: M \to N$に対してR-準同型$h: M \to L$があって$f = gh$であることを示せ．

41. Mが階数nの自由R-加群ならば，R-加群Nに対して

$$M \cong N \Leftrightarrow N \text{ も階数 } n \text{ の自由加群}$$

であることをを示せ.

42. Rは単項イデアル整域，Mは自由R-加群とする．M_1, M_2が$\{0\}$でないMの部分加群で$M=M_1 \oplus M_2$ならば，M_1, M_2共に自由加群で，Mの階数はM_1, M_2の階数の和であることを示せ.

43. Rは可換環，A, B, CはRのイデアルとする．$A+B=R$ならば$AB=A \cap B$を示せ．また，$A+B=B+C=C+A=R$ならば$ABC=A \cap B \cap C$を示せ.

44. $m_1, m_2, \cdots, m_n$は自然数で，$i \neq j$ならばm_i, m_jは互いに素であるとき$\bigcap_{i=1}^{n}(m_i)=(m_1 m_2 \cdots m_n)$を示せ.

45. R-加群Mに対してMからRへのR-準同型の全体をM^*とかく．$f, g \in M^*$, $a \in R$, $x \in M$に対して

$$(f+g)(x)=f(x)+g(x), \quad (fa)(x)=f(x) \cdot a$$

ときめて，M^*がR-右加群をつくることを示せ.

46. $\boldsymbol{Z}$-加群$\boldsymbol{Q}$の双対加群$\boldsymbol{Q}^*$は$\{0\}$であることを示せ.

47. Rが環，$A_1, A_2, \cdots, A_n$がRのイデアルで$R=A_i+A_j \ (i \neq j)$ならば，$R=A_i+\bigcap_{j \neq i} A_j$であることを示せ.

48. Rは単項イデアル整域，Mは階数有限の自由R-加群，NはMの部分加群$(\neq \{0\})$とする．このとき，次のことを示せ.

$$N \text{が} M \text{の直和因子} \Leftrightarrow M/N \text{が自由加群}.$$

49. Rを整域，MをR-加群とする．このとき，

$$t(M)=\{x \in M \mid \mathrm{Ann}_R\, x \neq \{0\}\}$$

はMの部分加群であることを示せ.

50. $\boldsymbol{Z}$-加群とみて$\boldsymbol{Q}$はトーション・フリー加群であることを示せ.

51. トーション加群の部分加群，剰余加群はトーション加群であることを示せ.

52. トーション・フリー加群の部分加群はトーション・フリー加群であるが，剰余加群はかならずしもそうでないことを示せ.

53. Rを整域，$M=Rx$を$\{0\}$でない巡回加群として，次のことを示せ.

(1) $t(M)=M \Leftrightarrow \mathrm{Ann}_R\, x \neq \{0\}$.　(2) $t(M)=\{0\} \Leftrightarrow \mathrm{Ann}_R\, x=\{0\}$.

54. Rを整域, M, NをR-加群, $f\colon M \to N$をR-準同型とする．このとき，次のことを示せ.

(1) $f(t(M)) \subseteqq t(N)$.　(2) fがR-同型ならば$f(t(M))=t(N)$.

55. Rを整域，MをR-加群とする．Mが部分加群M_1, M_2の内部直和ならば，$t(M)$は$t(M_1), t(M_2)$の内部直和であることを示せ．

56. Rが単項イデアル整域，Mが有限生成R-加群として，

$$M\text{がトーション・フリー加群} \Leftrightarrow M\text{が自由加群}$$

であることを示せ．

57. 位数32の同型でないアーベル群をすべて求めよ．

58. 加法群$\boldsymbol{Z}/(8)\oplus\boldsymbol{Z}/(12)$，$\boldsymbol{Z}/(4)\oplus\boldsymbol{Z}/(25)\oplus\boldsymbol{Z}/(100)$を$\boldsymbol{Z}/(a_1)\oplus\boldsymbol{Z}/(a_2)\oplus\cdots\oplus\boldsymbol{Z}/(a_n)$ ($a_1>1$，$a_i|a_{i+1}$，$1\leqq i\leqq n-1$) の形にあらわせ．

59. Gを有限アーベル群，pを素数とする．もしGの任意の元xに対して$px=0$ならば，Gは$(p, p, \cdots, p)$型のアーベル群であることを示せ．

60. Gを有限アーベル群，mを$|G|$の正の約数とすれば，Gは位数mの部分群をもつことを示せ．

4

体

この章では，体とその上の多項式について基本的な性質をのべる．これらは古典的な代数学の中心的な内容をなすもので，特に，体の代数拡大とその自己同型群との関係をのべたガロアの理論は，代数学の最も美しい理論の1つではあるが，ここでは触れない．また，最後の節の有限体の理論はコンピュータに広く応用されている．

4.1 拡 大 体

Kが体，kがKの部分体であるとき，Kをkの**拡大体**とよぶ．kを含むKの部分体をkとKの**中間体**とよぶ．

Kの部分集合Sに対して，kとKの中間体でSを含むものすべての共通部分はSを含むkとKの最小の中間体である．これをkにSを**添加した体**とよび，$k(S)$であらわす．特に，Sが有限集合$\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$であるときは$k(S)$を$k(\alpha_1, \alpha_2, \cdots, \alpha_n)$であらわす．

$S=\phi$のときは，kとKの中間体はすべてSを含むから

$$k(S)=k$$

が成り立つ．

$S\neq\phi$のときは，S'がSの有限部分集合のすべてをわたってつくった$k(S')$の和集合$\bigcup_{S'}k(S')$が$k(S)$に一致する．すなわち

$$k(S)=\bigcup_{S'}k(S').$$

実際，S'がSの部分集合であるから$k(S')\subseteqq k(S)$であり，したがって，$\bigcup_{S'}k(S')\subseteqq k(S)$となる．逆に，$\bigcup_{S'}k(S')$は$S$を含む$k$と$K$の中間体である

(この証明は演習問題とする) から，$k(S)$ の最小性により $k(S)=\bigcup_{S'}k(S')$ となる．

上のことから，特に，k に K の有限部分集合 S' を添加した体 $k(S')$ が基本的である．これをもう少し詳しくのべてみる．

まず，$S'=\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ とおき，k の元を係数とした $\alpha_1, \alpha_2, \cdots, \alpha_n$ の多項式

$$f(\alpha_1, \alpha_2, \cdots, \alpha_n)=\sum a_{i_1i_2\cdots i_n}\alpha_1{}^{i_1}\alpha_2{}^{i_2}\cdots\alpha_n{}^{i_n} \qquad (a_{i_1i_2\cdots i_n}\in k)$$

の全体を $k[\alpha_1, \alpha_2, \cdots, \alpha_n]$ とかく．$k[\alpha_1, \alpha_2, \cdots, \alpha_n]$ は k と $\alpha_1, \alpha_2, \cdots, \alpha_n$ を含む K の最小の部分環である．

$k[\alpha_1, \alpha_2, \cdots, \alpha_n]$ を含む K の部分体は，$\alpha_1, \alpha_2, \cdots, \alpha_n$ を含む k と K の中間体にほかならないから，$k[\alpha_1, \alpha_2, \cdots, \alpha_n]$ を含む K の最小の部分体 L は $\alpha_1, \alpha_2, \cdots, \alpha_n$ を含む k と K の最小の中間体 $k(\alpha_1, \alpha_2, \cdots, \alpha_n)$ に一致する．定理 2.7 によれば，L は次のように与えられる．

$$L=\{ab^{-1}\in K \mid a, b\in k[\alpha_1, \alpha_2, \cdots, \alpha_n], b\neq 0\}.$$

一方，$k[\alpha_1, \alpha_2, \cdots, \alpha_n]$ は体 K の部分環として整域であり，定理 2.9 から商体 M をもつが，2.4 節の最後に注意したように，M は L と一致すると考えた．したがって，次の定理が成り立つ．

定理 4.1　K を体 k の拡大体とする．K の有限個の元 $\alpha_1, \alpha_2, \cdots, \alpha_n$ に対して，次の 3 つの概念は一致する．

(1)　k に $\alpha_1, \alpha_2, \cdots, \alpha_n$ を添加した体 $k(\alpha_1, \alpha_2, \cdots, \alpha_n)$．

(2)　$k[\alpha_1, \alpha_2, \cdots, \alpha_n]$ を含む K の最小の部分体 L．

(3)　$k[\alpha_1, \alpha_2, \cdots, \alpha_n]$ の商体 M．

定理 4.1 の $k(\alpha_1, \alpha_2, \cdots, \alpha_n)$ を $\alpha_1, \alpha_2, \cdots, \alpha_n$ の k 上の**有理関数体**とよび，その元を $\alpha_1, \alpha_2, \cdots, \alpha_n$ の k 上の**有理式**とよぶ (2.5 節参照)．

K の 2 つの部分集合 S_1, S_2 に対して，k に S_1 を添加した体 $k(S_1)$ をまずつくり，$k(S_1)$ に S_2 を添加した体 $k(S_1)(S_2)$ をつくれば，

$$k(S_1)(S_2)=k(S_1\cup S_2)$$

が成り立つ．この証明は演習問題とする．

特に，体 $k(\alpha_1, \alpha_2, \cdots, \alpha_n)$ に対しては，上のことをくりかえし用いて

$$k(\alpha_1, \alpha_2, \cdots, \alpha_n)=k(\alpha_1, \alpha_2, \cdots, \alpha_{n-1})(\alpha_n)$$

$$=k(\alpha_1, \alpha_2, \cdots, \alpha_{n-2})(\alpha_{n-1})(\alpha_n)$$
$$= \cdots$$
$$=k(\alpha_1)(\alpha_2)\cdots(\alpha_n)$$

が成り立つ．このように k に K の有限個の元を添加するには，k に K のただ1個の元をくりかえし添加していけばよい．$k(\alpha)$ のようにただ1個の元を添加してえられる体を k の**単純拡大**とよぶ．

例 1 任意の体 K は素体 k の拡大体である (2.4 節例 2)．

例 2 $\boldsymbol{C}$ は $\boldsymbol{R}$ の拡大体である．$\boldsymbol{R}$ に $\boldsymbol{C}$ の元 i (虚数単位) を添加した体 $\boldsymbol{R}(i)$ は $\boldsymbol{C}$ と一致する．

実際，$\boldsymbol{R}(i)$ は $\boldsymbol{R}$ と i を含むから任意の複素数 $a+bi$ $(a, b \in \boldsymbol{R})$ を含んで $\boldsymbol{C}=\boldsymbol{R}(i)$ となる．

例 3 $\boldsymbol{R}$ は $\boldsymbol{Q}$ の拡大体である．$\boldsymbol{Q}$ に $\boldsymbol{R}$ の元 $\sqrt{2}$ を添加すると

$$\boldsymbol{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a, b \in \boldsymbol{Q}\}.$$

実際，右辺を L とかけば，L は $\boldsymbol{Q}$ と $\sqrt{2}$ を含む $\boldsymbol{R}$ の部分体である (演習問題2の12)．したがって．$\boldsymbol{Q}(\sqrt{2})$ の最小性から $\boldsymbol{Q}(\sqrt{2}) \subseteqq L$ である．$\boldsymbol{Q}(\sqrt{2})$ もまた $\boldsymbol{Q}$ と $\sqrt{2}$ を含むから，$a, b \in \boldsymbol{Q}$ ならば $a+b\sqrt{2} \in \boldsymbol{Q}(\sqrt{2})$ で $L \subseteqq \boldsymbol{Q}(\sqrt{2})$ が成り立つ．

$\boldsymbol{Q}(\sqrt{2}, \sqrt{3}) = \boldsymbol{Q}(\sqrt{2})(\sqrt{3})$ は

$$\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \mid a, b, c, d \in \boldsymbol{Q}\}$$

に等しく，$\boldsymbol{Q}(\sqrt{2}, \sqrt{3}) = \boldsymbol{Q}(\sqrt{2}+\sqrt{3})$ でもある (これらの証明は演習問題とする)．

4.2 単純拡大

K を体 k の拡大体とする．K の元 α が k 上**代数的**であるとは

$$\text{ある } f(x)(\neq 0) \text{ が } k[x] \text{ にあって } f(\alpha)=0$$

ときめる．代数的でない K の元を k 上**超越的**とよぶ．

補題 2.12 によれば，$k[x]$ から K への写像

$$h: k[x] \to K, \quad g(x) \to g(\alpha)$$

は環準同型で，その像 $h(k[x])$ を $k[\alpha]$ とかいた．$k[\alpha]$ は k の元を係数とする α の多項式の全体である．このとき

$$\alpha \text{ が } k \text{ 上超越的} \Leftrightarrow \operatorname{Ker} h = \{0\} \Leftrightarrow k[x] \cong^{h} k[\alpha]$$

を意味する．

定理 2.10 によれば，h は $k[x]$ の商体と $k[\alpha]$ の商体の間の同型写像にまで拡張できる．2.5 節で，$k[x]$ の商体を $k(x)$ とかき，k の上の x の有理関数体とよんだ．定理 4.1 から $k[\alpha]$ の商体は $k(\alpha)$ であるから，α が k 上超越的ならば，

$$k(x)\cong k(\alpha)$$

が成り立つ．特に，K の元 $\alpha, \beta, \cdots$ が k 上超越的ならば，

$$k(\alpha)\cong k(\beta)\cong\cdots$$

である．

逆に，全射準同型 $h: k[x]\to k[\alpha]$ を拡張して，商体の間の同型写像 $k(x)\cong k(\alpha)$ がえられるならば，h は単射，したがって，同型であって α は k 上超越的である．

これに対して，α が k 上代数的であることは $\mathrm{Ker}\,h\neq\{0\}$ を意味し，$k[x]$ が単項イデアル整域であるから (2.5 節例 4)，

$$\mathrm{Ker}\,h=(p(x))\qquad(p(x)\neq 0, p(x)\neq\text{定数})$$

をみたす $p(x)$ が $k[x]$ に存在する．$p(x)\neq 0$ は明らかであるが，$p(x)\neq$ 定数の証明は演習問題とする．

$p(x)$ はそのつくり方から，$\mathrm{Ker}\,h$ に属する 0 でない次数最小の多項式，すなわち，α を根とする 0 でない多項式の中で次数最小で，既約であり

$$g(x)\in k[x],\ g(\alpha)=0\ \Rightarrow\ p(x)\,|\,g(x)$$

をみたす．$g(x)\neq 0$ のときは

$$g(x)\in k[x],\ g(\alpha)=0\ \Rightarrow\ \deg g(x)\geqq\deg p(x)$$

である．補題 2.18 から $(p(x))$ は $k[x]$ の極大イデアル，2.3 節例 12 から $k[x]/(p(x))$ は体であることが分かる．このとき，$k[\alpha]$ も体で

$$k[\alpha]=k(\alpha)$$

が成り立つ．

実際，$k[\alpha]$ は k と a を含む K の最小の部分環であるから，α を含む k と K の中間体 $k(\alpha)$ に含まれる．しかし，$k[\alpha]$ が体をつくることは $k[\alpha]$ が k と K の中間体であることを意味し，$k(\alpha)$ の最小性から $k(\alpha)\subseteqq k[\alpha]$ をうる．

以上をまとめて

定理 4.2　K を体 k の拡大体とする．$\alpha\in K$ に対して

(1)　α が k 上超越的 $\Leftrightarrow$ 全射環準同型 $h: k[x]\to k[\alpha]$ を拡張して

$$k(x)\cong k(\alpha).$$

(2)　α が k 上代数的 $\Leftrightarrow$ α を根にもつ k 上の既約多項式 $p(x)$ があって

$$k[x]/(p(x))\cong k(\alpha).$$

例 1 $\boldsymbol{R}$ は $\boldsymbol{Q}$ の拡大体で，$\sqrt{2}\in\boldsymbol{R}$ に対して x^2-2 は $\sqrt{2}$ を根にもつ $\boldsymbol{Q}$ 上の既約多項式であるから，$\sqrt{2}$ は $\boldsymbol{Q}$ 上代数的であり

$$\boldsymbol{Q}(\sqrt{2})\cong\boldsymbol{Q}[x]/(x^2-2).$$

例 2 $\boldsymbol{Q}$ 上代数的な $\boldsymbol{C}$ の元を**代数的数**とよび，$\boldsymbol{Q}$ 上超越的な $\boldsymbol{C}$ の元を**超越数**とよぶ.

$\sqrt{2}$ は代数的数である．1873年エルミートは自然対数の底 e が，1882年にはリンデマンが円周率 π が超越数であることを証明した．したがって，

$$\boldsymbol{Q}(e)\cong\boldsymbol{Q}(\pi)\cong\boldsymbol{Q}(x)$$

が成り立つ.

K を体 k の拡大体とする．$\alpha\in K$ が k 上代数的ならば,

$$k[x]/(p(x))\overset{\bar{h}}{\cong}k[\alpha]=k(\alpha)$$

をみたす既約多項式 $p(x)\in k[x]$ が存在した．$p(x)$ は α を根とする 0 でない多項式の中で次数最小であった.

この $p(x)$ は定数多項式のちがいを除けば，α によって一意的にきまる.

実際，α を根にもつ 0 でない次数最小の多項式 $p'(x)$ をとし

$$p'(x)=p(x)q(x)+r(x)$$
$$(r(x)=0 \text{ または } \deg r(x)<\deg p(x))$$

とおけば，$p'(\alpha)=p(\alpha)=0$ から $r(\alpha)=0$．したがって，$r(x)=0$ で

$$p'(x)=p(x)q(x).$$

$p'(x)$ の次数最小性から $q(x)$ は定数多項式でなければならない.

この $p(x)$ を α の k 上の**最小多項式**とよぶ．普通は $p(x)$ をその最高次係数で割ってモニックな多項式としたものを，改めて $p(x)$ とかく．このとき，$p(x)$ は α によって一意的にきまる．$p(x)$ の次数を α の k 上の**次数**とよぶ.

例 3 $\alpha=\sqrt{2}$ は $\boldsymbol{Q}$ 上代数的で，$\boldsymbol{Q}$ 上の最小多項式は $p(x)=x^2-2$ である.

例 4 $\alpha=\sqrt{2}+i$ では両辺を平方して $\alpha^2=1+2\sqrt{2}i$．これを $\alpha^2-1=2\sqrt{2}i$ と変形し，再び平方すると

$$\alpha^4-2\alpha^2+9=0.$$

したがって，α は $\boldsymbol{Q}$ 上代数的であるが，α を根にもつ 0 でない $\boldsymbol{Q}$ 上の多項式で x^4-2x^2+9 より次数の低いものはない.

実際，$ax^2+bx+c\in\boldsymbol{Q}[x]$ が α を根にもつならば,

$$a(\sqrt{2}+i)^2+b(\sqrt{2}+i)+c=0,$$

$$(a+\sqrt{2}b+c)+(2\sqrt{2}a+b)i=0$$

から $a+\sqrt{2}b+c=2\sqrt{2}a+b=0$ をうるが，$b=-2\sqrt{2}a$ は $\boldsymbol{Q}$ の元ではありえない．3次の多項式の場合も同じで（この証明は演習問題とする），

$$p(x)=x^4-2x^2+9$$

が α の $\boldsymbol{Q}$ 上の最小多項式である．

これに対して，α の $\boldsymbol{R}$ 上の最小多項式は

$$p(x)=x^2-2\sqrt{2}x+3$$

である．

例 5　$\boldsymbol{C}$ は $\boldsymbol{Q}$ の拡大体であり，この $\boldsymbol{Q}$ に $\boldsymbol{C}$ の元 ω, ω^2 を添加する．ここで $\omega=\dfrac{-1+\sqrt{3}i}{2}$ は1の3乗根をあらわす．$\omega^2+\omega+1=0$ から $\omega^2=-1-\omega\in\boldsymbol{Q}(\omega)$ で，$\boldsymbol{Q}(\omega^2)\subseteqq\boldsymbol{Q}(\omega)$ が成り立つ．また $\omega=-1-\omega^2$ であるから $\boldsymbol{Q}(\omega)\subseteqq\boldsymbol{Q}(\omega^2)$ でもある．したがって，

$$\boldsymbol{Q}(\omega)=\boldsymbol{Q}(\omega^2).$$

このことは相異なる元を添加しても同じ拡大体がえられることを示している．

ω, ω^2 は共に1の3乗根であるから $\boldsymbol{Q}$ 上代数的である．$\omega^2+\omega+1=0$ から ω の $\boldsymbol{Q}$ 上の最小多項式は

$$p(x)=x^2+x+1$$

である．一方，$\omega^3=1$ に注意すれば，

$$\omega^4+\omega^2+1=\omega+\omega^2+1=0$$

でもあるから，$p(x)=x^2+x+1$ は ω^2 の $\boldsymbol{Q}$ 上の最小多項式でもある．したがって，

$$\boldsymbol{Q}[x]/(x^2+x+1)\cong^{\bar{h}}\boldsymbol{Q}[\omega]=\boldsymbol{Q}(\omega)=\boldsymbol{Q}(\omega^2)$$

が成り立つ．このことは単純拡大 $k(\alpha)$ の構造が，α よりも α の最小多項式によってきまることを示している．

次の補題はしばしば有用である．

補題 4.3　k を体，$f(x)\in k[x]$ を n 次の既約多項式，α を k のある拡大体における $f(x)$ の根とする．このとき α は k 上代数的で，その k 上の次数は n に等しい．

証明　明らかに α は k 上代数的で，その k 上の最小多項式を $p(x)$，$p(x)$ の次数を m とおく．$m\leqq n$ であり，$p(x)\mid f(x)$ であるから

$$f(x)=p(x)q(x)$$

をみたす $q(x)\in k[x]$ が存在するが，$f(x)$ の既約性から $q(x)$ は定数多項式でなければならない．したがって，$m=n$ となる．

k を体，$f(x)\in k[x]$ を n 次の既約多項式，α を k のある拡大体における $f(x)$ の根とする．α は k 上代数的であり，k 上の次数は n である．

$k(\alpha)=k[\alpha]$ であるから，$k(\alpha)$ の任意の元は

ある $g(x)\in k[x]$ であって，$g(\alpha)$ の形

にあらわされる．$g(x)$ を $f(x)$ で割って

$$g(x)=f(x)q(x)+r(x)$$
$$(r(x)=0 \text{ または } \deg r(x)<n)$$

とかく．x に α を代入して

$$g(\alpha)=f(\alpha)q(\alpha)+r(\alpha)=r(\alpha).$$

$r(x)=0$ のときは，$g(\alpha)=r(\alpha)=0$ である．$r(x)\neq 0$ のときは，

$$r(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1} \qquad (a_i\in k,\ 0\leqq i\leqq n-1)$$

とかける．したがって，$g(\alpha)$ は

$$g(\alpha)=r(\alpha)=a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}$$

とあらわされる．このとき，もし $g(\alpha)$ が

$$g(\alpha)=a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}=b_0+b_1\alpha+\cdots+b_{n-1}\alpha^{n-1}$$

と二通りにあらわされるならば，

$$(a_0-b_0)+(a_1-b_1)\alpha+\cdots+(a_{n-1}-b_{n-1})\alpha^{n-1}=0$$

となり，α の k 上の次数が n であることに矛盾する．したがって，

定理 4.4 k を体，$f(x)\in k[x]$ を n 次の既約多項式とする．k のある拡大体における $f(x)$ の根 α に対して，$k(\alpha)$ の 0 でない元は

$$a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1} \qquad (a_i\in k, 0\leqq i\leqq n-1)$$

の形に一意的にあらわされる．

例 6 $\boldsymbol{R}$ の上の多項式 x^2+1 は 2 次の既約多項式であり，$\boldsymbol{R}$ の拡大体 $\boldsymbol{C}$ に根 i (虚数単位) をもつ．i の $\boldsymbol{R}$ 上の最小多項式は x^2+1 であり，i の $\boldsymbol{R}$ 上の次数は 2 である．定理 4.4 から

$$\boldsymbol{R}(i)=\{a+bi \mid a, b\in\boldsymbol{R}\}=\boldsymbol{C}$$

が成り立つ．同じように考えて

$$\boldsymbol{Q}(\sqrt{2})=\{a+b\sqrt{2} \mid a, b\in\boldsymbol{Q}\},$$
$$\boldsymbol{Q}(\omega)=\{a+b\omega \mid a, b\in\boldsymbol{Q}\}$$

をうる.

Kが体kの拡大体で，Kの元$\alpha_1, \alpha_2, \cdots, \alpha_n$は$k$上代数的とする．まず，

$$k(\alpha_1)=k[\alpha_1]$$

である．α_2はk上代数的であるから，$k(\alpha_1)$上代数的で

$$k(\alpha_1, \alpha_2)=k(\alpha_1)(\alpha_2)=k(\alpha_1)[\alpha_2]=(k[\alpha_1])[\alpha_2]=k[\alpha_1, \alpha_2]$$

が成り立つ．以下同じようにして

$$k(\alpha_1, \alpha_2, \cdots, \alpha_n)=k[\alpha_1, \alpha_2, \cdots, \alpha_n]$$

が成り立つ．すなわち，$k(\alpha_1, \alpha_2, \cdots, \alpha_n)$の元は$k$の元を係数とする$\alpha_1, \alpha_2, \cdots, \alpha_n$の多項式としてかけることが分かる.

これまでは体kとその拡大体Kがあり，Kの元αがk上のある既約多項式の根である場合を考えてきた.

ここでは，逆に，k上の任意の既約多項式がkのある拡大体Kに根をもつことを確かめる．このことが分かれば，0でも定数でもない多項式はいくつかの既約多項式の積に分解される(2.6節例10)から，既約多項式にかぎらずk上の0でも定数でもない多項式もkのある拡大体Kに根をもつことが分かる.

k上の既約多項式を

$$f(x)=a_0+a_1x+\cdots+a_nx^n$$

とする．$f(x)$は$k[x]$の素元であり，したがって，剰余環

$$k[x]/(f(x))$$

は体である．この体をKとかき，写像φを

$$\varphi\colon k\to K, \quad a\to \bar{a}=a+(f(x))$$

ときめる．φは一意写像であり単射環準同型であって，aと$\bar{a}$を同一視してKをkの拡大体とみることができる.

実際，φが一意写像で環準同型であることは明らか．φが単射であることをみるために$a+(f(x))=\bar{0}$とおく．$a=f(x)q(x)$をみたす$q(x)\in k[x]$が存在する．もし$q(x)\neq 0$ならば，$\deg q(x)$が考えられ，$\deg f(x)\geqq 1$, $\deg q(x)\geqq 0$から右辺の次数$\geqq 1$であるのに，左辺の次数$=0$で矛盾である．したがって，$q(x)=0, a=0$である.

$\bar{x}=x+(f(x))$はKの元で，これをαとかけば，

$$\bar{0}=\overline{f(x)}=\bar{a}_0+\bar{a}_1\bar{x}+\cdots+\bar{a}_n\bar{x}^n=\bar{a}_0+\bar{a}_1\alpha+\cdots+\bar{a}_n\alpha^n.$$

ここでkの元aとKの元$\bar{a}$とを同一視すれば，

$$0=\bar{0}=\bar{a}_0+\bar{a}_1\alpha+\cdots+\bar{a}_n\alpha^n=a_0+a_1\alpha+\cdots+a_n\alpha^n=f(\alpha)$$

となり，α が $f(x)$ の根であることが分かる．

K の任意の元は，ある $g(x)\in k[x]$ があって，$\overline{g(x)}$ とあらわされる．上と同じようにして

$$\overline{g(x)}=g(\alpha)\in k[\alpha]=k(\alpha)$$

が成り立ち，$K=k(\alpha)$ をうる．

以上をまとめて

定理 4.5 k を体，$f(x)$ を k 上の既約多項式とする．$f(x)$ は k の拡大体 $k[x]/(f(x))$ に1つの根 α をもち，$k[x]/(f(x))=k(\alpha)$ が成り立つ．

例 7 $k=\boldsymbol{Z}/(2)$ の上で $f(x)=x^3+x+1$ は既約多項式である (2.6節例8)．$f(x)$ は k の拡大体 $K=k[x]/(f(x))$ に根 α をもつ．$K=k(\alpha)$ でもあるから定理4.4によって

$$\begin{aligned}K&=\{a+b\alpha+c\alpha^2 \mid a,b,c\in k\}\\&=\{0,1,\alpha,1+\alpha,\alpha^2,1+\alpha^2,\alpha+\alpha^2,1+\alpha+\alpha^2\}\end{aligned}$$

で，K は8個の元からなる体である．

この K の演算の例として，$1+\alpha+\alpha^2$ の逆元を求めてみよう．

$$(1+\alpha+\alpha^2)(a+b\alpha+c\alpha^2)=1 \qquad (a,b,c\in k)$$

とおけば，

$$a+(a+b)\alpha+(a+b+c)\alpha^2+(b+c)\alpha^3+c\alpha^4=1.$$

$\alpha^3+\alpha+1=0$ からは $\alpha^3=-(1+\alpha)$ をうる．K の任意の元 β に対して，$\beta+\beta=(1+1)\beta=0$ (1は k の単位元) であるから，$\beta=-\beta$ が成り立ち，したがって，$\alpha^3=-(1+\alpha)=1+\alpha$ であり，$\alpha^4=\alpha(1+\alpha)=\alpha+\alpha^2$ である．これを上の式に代入して

$$a+(a+b)\alpha+(a+b+c)\alpha^2+(b+c)(1+\alpha)+c(\alpha+\alpha^2)=1,$$
$$(a+b+c)+a\alpha+(a+b)\alpha^2=1$$

となる．

$$a+b+c=1, \quad a=0, \quad a+b=0$$

から $a=b=0$, $c=1$ で

$$(1+\alpha+\alpha^2)^{-1}=\alpha^2.$$

例 8 $k=\boldsymbol{R}$ の上で $f(x)=x^2+1$ は既約多項式である．$f(x)$ は k の拡大体 $K=k[x]/(f(x))$ に根 α をもつ．$K=k(\alpha)$ でもあるから

$$K=\{a+b\alpha \mid a,b\in k\}.$$

K では2元の和は

$$(a+b\alpha)+(c+d\alpha)=(a+c)+(b+d)\alpha$$

で与えられ，2元の積は $\alpha^2=-1$ に注意して

$$(a+b\alpha)(c+d\alpha)=(ac-bd)+(ad+bc)\alpha$$

で計算される．このとき写像 φ を

$$\varphi: \boldsymbol{C} \to K, \quad a+bi \to a+b\alpha$$

ときめる．φ は一意写像であり環同型でもある．

$f(x)$ は K では

$$x^2+1=x^2-\alpha^2=(x-\alpha)(x+\alpha)$$

と分解される．$f(x)$ は k の別の拡大体 $\boldsymbol{C}$ では

$$x^2+1=(x-i)(x+i)$$

と分解される．

K では $k(\alpha)=K$, $\boldsymbol{C}$ では $k(i)=\boldsymbol{C}$ が成り立つ．$f(x)$ の根をもつ k の拡大体が $K, \boldsymbol{C}$ と2つあっても，この2つが環同型であることはもっと一般に成り立つ(定理 4.13 参照)．

後の節のために補題を1つ準備する．

$k, \bar{k}$ は体，$\varphi: k \to \bar{k}$ を環同型とする．このとき，多項式環 $k[x]$ から $\bar{k}[x]$ への環同型 φ_1 を

$$\varphi_1: k[x] \to \bar{k}[x], \quad g(x)=\sum a_i x^i \to \bar{g}(x)=\sum \varphi(a_i)x^i$$

ときめれば，k への制限写像 $\varphi_1|_k$ が φ に等しい．

したがって，図 4.1 の図型は可換となる．ここで $\subseteqq$ は包含写像をあらわす．

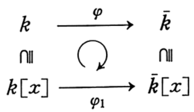


図 4.1

φ_1 が一意写像であり，環同型でもあることの証明は演習問題とする．

φ_1 が環同型であるから，$g(x) \in k[x]$ が可約ならば $\bar{g}(x)$ も可約となる．したがって，

$$g(x) \text{ が既約} \Leftrightarrow \bar{g}(x) \text{ が既約}$$

が成り立つ．この証明も演習問題とする．

補題 4.6　$k, \bar{k}$ は体，$\varphi: k \to \bar{k}$ は環同型とする．$f(x)$ を k 上の既約多項式，α を $f(x)$ の1つの根とする．このとき，$\bar{\alpha}$ が $\bar{f}(x)=\varphi_1(f(x))$ の根ならば，

環同型

$$\varphi_2\colon k(\alpha)\to \bar{k}(\bar{\alpha})$$

があって，$\varphi_2|_k=\varphi$ で $\varphi_2(\alpha)=\bar{\alpha}$ が成り立つ．

$$\begin{array}{ccc} k & \xrightarrow{\ \varphi\ } & \bar{k} \\ \cap\!\shortparallel & \circlearrowright & \cap\!\shortparallel \\ k(\alpha) & \xrightarrow[\varphi_2]{} & \bar{k}(\bar{\alpha}) \end{array}$$

図 4.2

証明　$f(x)$ が n 次ならば $\bar{f}(x)$ も n 次の既約多項式であるから，$k(\alpha)$，$\bar{k}(\bar{\alpha})$ の 0 でない元はそれぞれ

$$a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1},\quad \varphi(b_0)+\varphi(b_1)\bar{\alpha}+\cdots+\varphi(b_{n-1})\bar{\alpha}^{n-1}$$
$$(a_i, b_i\in k,\ 0\leqq i\leqq n-1)$$

と一意的にあらわされるので（定理 4.4），φ_2 を

$$\varphi_2\colon k(\alpha)\to\bar{k}(\bar{\alpha}),$$
$$a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}\to\varphi(a_0)+\varphi(a_1)\bar{\alpha}+\cdots+\varphi(a_{n-1})\bar{\alpha}^{n-1}$$

ときめればよい．

例 9　補題 4.6 で $k=\bar{k}=\boldsymbol{Q}$，$\varphi=1_{\boldsymbol{Q}}$ とする．$f(x)=x^3-2$ は $\boldsymbol{Q}$ の上の既約多項式（2.6 節例 14）で，$\boldsymbol{R}$ に根 $\alpha=\sqrt[3]{2}$ をもつ．$\sqrt[3]{2}\,\omega$ は $\bar{f}(x)=f(x)$ の $\boldsymbol{C}$ における根で，補題 4.6 の環同型 φ_2 は

$$\varphi_2\colon(\boldsymbol{Q}\sqrt[3]{2})\to\boldsymbol{Q}(\sqrt[3]{2}\,\omega),\quad a_0+a_1\alpha+a_2\alpha^2\to a_0+a_1\alpha\omega+a_2\alpha^2\omega^2$$

で与えられる．

4.3　有限拡大と代数拡大

K を体 k の拡大体とする．K は加法群であり，$k\times K$ から K への写像を

$$(a, x)\to a\ と\ x\ の\ K\ における積\ ax$$

ときめて，K を自然に k-加群，したがって，k 上の左ベクトル空間とみることができる．このとき，K の k 上の次元が有限ならば，K を k の**有限次拡大体**または単に**有限拡大**とよぶ．K の k 上の次元を $[K:k]$ とかき，K の k 上の**拡大次数**または単に**次数**とよぶ．

$\alpha\in K$ が k 上代数的ならば，k 上の α の最小多項式

$$p(x)=a_0+a_1x+\cdots+a_nx^n$$

は α を根とする 0 でない多項式の中で次数最小である．$p(x)\neq 0$ で

$$0=p(\alpha)=a_0+a_1\alpha+\cdots+a_n\alpha^n$$

であることは $1, \alpha, \alpha^2, \cdots, \alpha^n$ が k 上1次従属であることを意味する．また，$p(x)$ の次数最小性から

$$\text{ある } b_0, b_1, \cdots, b_{n-1}\in k \text{ があって } b_0+b_1\alpha+\cdots+b_{n-1}\alpha^{n-1}=0$$
$$\Rightarrow b_0=b_1=\cdots=b_{n-1}=0$$

であるから，$1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ は k 上1次独立である．

その上，定理 4.4 から $k(\alpha)$ の 0 でない元は，ある $g(x)\in k[x]$ があって

$$g(\alpha)=c_0+c_1\alpha+\cdots+c_{n-1}\alpha^{n-1}$$

の形に一意的にあらわされる．したがって，$k(\alpha)$ を k 上のベクトル空間とみて

$$1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$$

が $k(\alpha)$ の k 上の基底をつくる．$k(\alpha)$ は k の有限拡大で $[k(\alpha):k]=n$ である．

逆に，$k(\alpha)$ が k の有限拡大で，$[k(\alpha):k]=n$ ならば，$k(\alpha)$ の元 α に対して $1, \alpha, \alpha^2, \cdots, \alpha^n$ なる $(n+1)$ 個の $k(\alpha)$ の元は k 上1次独立ではありえないから，α は k 上代数的となる．

定理 4.7　K が体 k の拡大体で，$\alpha\in K$ であるとき，

$$\alpha \text{ が } k \text{ 上代数的} \Leftrightarrow k(\alpha) \text{ が } k \text{ の有限拡大}.$$

このとき，$[k(\alpha):k]$ は α の k 上の次数に等しく，これを n とかけば，

$$1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$$

が $k(\alpha)$ の k 上の基底をつくる．

例 1　$\boldsymbol{R}$ は $\boldsymbol{Q}$ の拡大体で，$\sqrt{2}\in\boldsymbol{R}$ は $\boldsymbol{Q}$ 上代数的で，その最小多項式は x^2-2 であった (4.2 節例 3)．したがって，$1, \sqrt{2}$ が $\boldsymbol{Q}(\sqrt{2})$ の $\boldsymbol{Q}$ 上の基底で $[\boldsymbol{Q}(\sqrt{2}):\boldsymbol{Q}]=2$ となる．このことから

$$\boldsymbol{Q}(\sqrt{2})=\{a+b\sqrt{2} \mid a, b\in\boldsymbol{Q}\}$$

が成り立つ (4.1 節例 2)．

例 2　$\alpha=1+\sqrt{2}+\sqrt{3}\in\boldsymbol{R}$ は $\boldsymbol{Q}$ 上代数的で，その最小多項式は

$$x^4-4x^3-4x^2+16x-8$$

である (この証明は演習問題とする)．したがって，$[\boldsymbol{Q}(\alpha):\boldsymbol{Q}]=4$ で $1, \alpha, \alpha^2, \alpha^3$ が $\boldsymbol{Q}(\alpha)$ の $\boldsymbol{Q}$ 上の基底をつくる．

$\sqrt{2}+\sqrt{3}=\alpha-1\in\boldsymbol{Q}(\alpha)$ であり，$\sqrt{3}-\sqrt{2}=\dfrac{1}{\sqrt{2}+\sqrt{3}}$ もまた $\boldsymbol{Q}(\alpha)$ に属するから，$\sqrt{2}, \sqrt{3}$ も $\boldsymbol{Q}(\alpha)$ に属する．

$\sqrt{2}, \sqrt{3}$ を上の基底であらわしてみよう．

$$\frac{1}{\alpha-1}=a\alpha^3+b\alpha^2+c\alpha+d \qquad (a, b, c, d\in\boldsymbol{Q})$$

とおく．分母を払って $(a\alpha^3+b\alpha^2+c\alpha+d)(\alpha-1)=1$． この式に $\alpha^4=4\alpha^3+4\alpha^2-16\alpha+8$ を代入すると

$$(3a+b)\alpha^3+(4a-b+c)\alpha^2-(16a+c-d)\alpha+(8a-d-1)=0.$$

これから $3a+b=4a-b+c=16a+c-d=8a-d-1=0$ で

$$a=-1,\quad b=3,\quad c=7,\quad d=-9$$

をうる．したがって，

$$\sqrt{3}=\frac{1}{2}\left(\alpha-1+\frac{1}{\alpha-1}\right)=-\frac{1}{2}(\alpha^3-3\alpha^2-8\alpha+10),$$

$$\sqrt{2}=\alpha-1-\sqrt{3}=\frac{1}{2}(\alpha^3-3\alpha^2-6\alpha+8).$$

Kを体 k の拡大体とする．Kのすべての元が k 上代数的ならば，Kを k の**代数的拡大体**または単に**代数拡大**とよぶ．

Kが k の有限拡大で $[K:k]=n$ ならば，Kの任意の元 α に対して

$$1, \alpha, \alpha^2, \cdots, \alpha^n$$

は k 上1次従属，したがって，α は k 上代数的である．すなわち，

$$K\text{が }k\text{ の有限拡大} \Rightarrow K\text{は }k\text{ の代数拡大}$$

である．特に

$$\begin{aligned} k(\alpha)\text{ が }k\text{ の有限拡大} &\Rightarrow k(\alpha)\text{ は }k\text{ の代数拡大} \\ &\Rightarrow \alpha\text{ は }k\text{ 上代数的} \end{aligned}$$

であるから，定理4.7により

(1) $k(\alpha)$ が k の有限拡大，

(2) $k(\alpha)$ が k の代数拡大，

(3) α が k 上代数的

の3つの概念は同値となるが，一般には代数拡大はかならずしも有限拡大ではない (例6参照).

例 3 虚数単位 i は $\boldsymbol{R}$ 上代数的で $\boldsymbol{C}=\boldsymbol{R}(i)$ であった (4.2節例6)． 定理4.7から $\boldsymbol{C}$ は $\boldsymbol{R}$ の有限拡大であり，したがって，$\boldsymbol{R}$ の代数拡大である．すなわち，複素数はすべて $\boldsymbol{R}$ 上代数的である．

定理 4.8 Kが体 k の拡大体，LがKの拡大体ならば，Lは k の拡大体であって

$$L\text{が }k\text{ の有限拡大} \Leftrightarrow K\text{が }k\text{ の，}L\text{が}K\text{の有限拡大}.$$

このとき

$$[L:k]=[L:K]\cdot[K:k].$$

証明　L が k の拡大体であることは補題2.3から明らか．したがって，L は k 上のベクトル空間になっている．

L が k の有限拡大とする．$k\subseteqq K\subseteqq L$ で，k の元と K の元との積は K に属するから K は L の k-部分空間である．したがって，$[K:k]\leqq[L:k]$ で K は k の有限拡大である．

L の元 $\alpha_1, \alpha_2, \cdots, \alpha_n$ が k 上1次従属ならば K 上1次従属であるから，対偶をとって，$\alpha_1, \alpha_2, \cdots, \alpha_n$ が K 上1次独立ならば k 上1次独立である．したがって，$n\leqq[L:k]$ で L は K の有限拡大である．

逆に，K が k の，L が K の有限拡大として K の k 上の基底を $\alpha_1, \alpha_2, \cdots, \alpha_n$，$L$ の K 上の基底を $\beta_1, \beta_2, \cdots, \beta_m$ とかく．$\alpha_i\beta_j$ $(1\leqq i\leqq n,\ 1\leqq j\leqq m)$ が k 上の L の基底となるから，L は k 上有限拡大であり，このとき $[L:k]=[L:K]\cdot[K:k]$ も成り立つ．

例 4　$\boldsymbol{Q}(\sqrt{2})=\{a+b\sqrt{2}\mid a, b\in\boldsymbol{Q}\}$ は $\boldsymbol{Q}$ の有限拡大で $[\boldsymbol{Q}(\sqrt{2}):\boldsymbol{Q}]=2$ である．演習問題3から

$$\begin{aligned}\boldsymbol{Q}(\sqrt{2}, \sqrt{3})&=\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\mid a, b, c, d\in\boldsymbol{Q}\}\\&=\{(a+b\sqrt{2})+(c+d\sqrt{2})\sqrt{3}\mid a+b\sqrt{2}, c+d\sqrt{2}\\&\qquad\in\boldsymbol{Q}(\sqrt{2})\}.\end{aligned}$$

$\boldsymbol{Q}(\sqrt{2}, \sqrt{3})=\boldsymbol{Q}(\sqrt{2})(\sqrt{3})$ は $\boldsymbol{Q}(\sqrt{2})$ の有限拡大で $[\boldsymbol{Q}(\sqrt{2}, \sqrt{3}):\boldsymbol{Q}(\sqrt{2})]$ も2に等しい．したがって，

$$[\boldsymbol{Q}(\sqrt{2}, \sqrt{3}):\boldsymbol{Q}]=[\boldsymbol{Q}(\sqrt{2}, \sqrt{3}):\boldsymbol{Q}(\sqrt{2})]\cdot[\boldsymbol{Q}(\sqrt{2}):\boldsymbol{Q}]=4.$$

定理 4.9　K が体 k の拡大体であるとき，

K が k の有限拡大 $\Leftrightarrow$ k 上代数的な有限個の K の元 $\alpha_1, \alpha_2, \cdots, \alpha_n$ があって

$$K=k(\alpha_1, \alpha_2, \cdots, \alpha_n).$$

証明　K を k の有限拡大，K の k 上の基底を $\alpha_1, \alpha_2, \cdots, \alpha_n$ とする．K の元は $a_1\alpha_1+a_2\alpha_2+\cdots+a_n\alpha_n$ $(a_i\in k)$ の形にかけるから $K=k(\alpha_1, \alpha_2, \cdots, \alpha_n)$ が成り立つ．有限拡大は代数拡大であるから，α_i は k 上代数的である．

逆に，$\alpha_1, \alpha_2, \cdots, \alpha_n$ が k 上代数的で，$K=k(\alpha_1, \alpha_2, \cdots, \alpha_n)$ とする．$k(\alpha_1)$ は k の有限拡大，α_2 は $k(\alpha_1)$ 上代数的でもあるから，$k(\alpha_1, \alpha_2)=k(\alpha_1)(\alpha_2)$ は $k(\alpha_1)$ の有限拡大，したがって，k の有限拡大である．このことをくりかえして，$k(\alpha_1, \alpha_2, \cdots, \alpha_n)$ は k の有限拡大である．

例 5　Kが体kの拡大体であるとき，

$$L=\{\alpha\in K \mid \alpha \text{は} k \text{上代数的}\}$$

はkとKの中間体で，kの代数拡大である．その上，Kの元でL上代数的なものはLの元にかぎられる．

実際，Lはkを含むKの部分集合であり，Lの2元α_1, α_2に対して，$k(\alpha_1, \alpha_2)$はkの有限拡大，したがって，kの代数拡大である．$\alpha_1-\alpha_2$も$\alpha_1\alpha_2^{-1}$($\alpha_2\neq 0$のとき)も$k(\alpha_1, \alpha_2)$に属するからk上代数的であり，またLに属する．補題2.3によりLはKの部分体をつくる．

Lの元はすべてk上代数的であるから，Lはkの代数拡大である．

最後に，$\alpha\in K$がL上代数的ならば，$L(\alpha)$がLの代数拡大である．Lがkの代数拡大であるから$L(\alpha)$がkの代数拡大となり(定理4.11参照)，したがって，αはk上代数的，$\alpha\in L$となる．

このLをkのKにおける**代数的閉包**とよぶ．これがkに一致するとき，kはKにおいて**代数的に閉じている**という．特に，kの代数拡大がkにかぎられるとき，すなわち，kは任意の拡大体において代数的に閉じているとき，kを**代数的閉体**とよぶ．代数的閉体については，その上の多項式の根に関連して2.5節で触れたが，ここで次の定理をあげておく．

定理 4.10　体kについて次の条件は同値である．

(1)　kは代数的閉体である．

(2)　$k[x]$の既約多項式は1次式である．

(3)　$k[x]$の定数でない多項式は1次式の積としてあらわされる．

(4)　$k[x]$の定数でない多項式はkに少なくとも1個の根をもつ．

証明　(1) ⇒ (4)：$k[x]$の定数でない多項式を$f(x)$とし，$f(x)$を$k[x]$で既約多項式の積としてあらわし，そこにあらわれる既約多項式の1つを$p(x)$とする．

定理4.5から$p(x)$は，したがって，$f(x)$はkの適当な拡大体Kに1つの根αをもつ．$k(\alpha)$はkの代数拡大であるから，仮定により，$k(\alpha)=k$で，$\alpha\in k$となって$f(x)$はkに1つの根をもつ．

(4) ⇒ (3)：定数でない多項式を$f(x)$とかき，$f(x)$の次数に関する帰納法で証明したらよい．この証明は演習問題とする．

(3) ⇒ (2)は明らか．

(2) ⇒ (1)：kの拡大体Kがk上代数的とする．Kの任意の元αはk上代数的

で，その k 上の最小多項式 $p(x)$ は仮定から1次式となる．$p(x)=ax+b$ $(a, b \in k)$ とかけば $0=p(\alpha)=a\alpha+b$ であるから $\alpha=-\dfrac{b}{a}\in k$ をうる．したがって，$K=k$ でなければならない．

例 6　例5で，特に，$K=\boldsymbol{C}, k=\boldsymbol{Q}$ のとき，L は

$$L=\{\alpha\in\boldsymbol{C} \mid \alpha \text{ は代数的数}\}$$

となる．L は $\boldsymbol{Q}$ の代数拡大ではあるが，有限拡大ではない．

実際，L が $\boldsymbol{Q}$ の有限拡大であるとして $[L:\boldsymbol{Q}]=n$ とおく．素数 p に対して

$$f(x)=x^{n+1}+p$$

は $\boldsymbol{Q}$ で既約である (2.6節例14)．定理2.16から $f(x)$ は $\boldsymbol{C}$ に少なくとも1つの根 α をもつ．α は $\boldsymbol{Q}$ 上代数的であり，その次数は $n+1$ に等しい (補題4.3)．定理4.7によって $[\boldsymbol{Q}(\alpha):\boldsymbol{Q}]=n+1$ であるが，

$$n=[L:\boldsymbol{Q}]\geqq[\boldsymbol{Q}(\alpha):\boldsymbol{Q}]=n+1$$

となって矛盾である．

定理 4.11　K が体 k の拡大体，L が K の拡大体とする．このとき，L は k の拡大体であって

$$L \text{ が } k \text{ の代数拡大} \Leftrightarrow K \text{ が } k \text{ の，} L \text{ が } K \text{ の代数拡大．}$$

証明　$\Rightarrow$ は明らかで，$\Leftarrow$ のみ示す．L の任意の元 α は K の元 $\beta_0, \beta_1, \cdots, \beta_n$ を係数とする多項式 $\beta_0+\beta_1x+\cdots+\beta_nx^n$ の根である．各 β_i は k 上代数的で $k(\beta_0, \beta_1, \cdots, \beta_n)$ は k の有限拡大である (定理4.9)．α は $k(\beta_0, \beta_1, \cdots, \beta_n)$ 上代数的であるから，$k(\beta_0, \beta_1, \cdots, \beta_n, \alpha)=k(\beta_0, \beta_1, \cdots, \beta_n)(\alpha)$ は $k(\beta_0, \beta_1, \cdots, \beta_n)$ の有限拡大，したがって，k の有限拡大でもある．α は k 上代数的である．

4.4 分解体

2.5節例6で $\boldsymbol{R}$ の上の定数でない多項式は $\boldsymbol{C}$ において1次式の積に分解されることをのべた．このことを一般的にのべると

定理 4.12　体 k 上の n $(\geqq 1)$ 次の多項式 $f(x)$ に対して，k の拡大体 K があって $f(x)$ は K において1次式の積に分解される．すなわち，

$$K \text{ の元 } \alpha_1, \alpha_2, \cdots, \alpha_n \text{ と } k \text{ の元 } a \text{ があって}$$

$$f(x)=a\cdot(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$

とあらわされる．したがって，$f(x)$ は K の中に (重複を数えて) きっちり n 個の根をもつ．

定理 2.15 では $f(x)$ は k の中に n 個より多くの根をもちえないことを示したが，定理 4.12 は k の適当な拡大体までひろげれば，そこにすべての根が存在することを示している．

定理 4.12 の**証明**　n に関する帰納法で証明する．

$n=1$ のときは，$K=k$ とおけばよい．

$n>1$ とし，n より次数の低い多項式に対しては定理は正しいと仮定する．まず，$f(x)$ を $k[x]$ で既約多項式の積であらわし，その 1 つの既約多項式を $p(x)$ とする．定理 4.5 から k の適当な拡大体 L があって，$p(x)$ は L の中に 1 つの根 α_1 をもつ．α_1 は $f(x)$ の根でもあり $L[x]$ で補題 2.14 を用いて

$$f(x)=(x-\alpha_1)q(x)$$

とあらわす．$q(x)$ の次数は $n-1$ であるから，帰納法の仮定で，L の，したがって，k の拡大体 K があって，K において

$$q(x)=a\cdot(x-\alpha_2)\cdots(x-\alpha_n) \qquad (a, \alpha_2, \cdots, \alpha_n \in K)$$

と 1 次式の積にあらわされ

$$f(x)=a\cdot(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$

となる．両辺の係数を比べて a が $f(x)$ の最高次係数で，$a\in k$ であることも分かる．

ここで，$\alpha_1, \alpha_2, \cdots, \alpha_n$ は $f(x)$ の K における根である．もし $\alpha\in K$ が $f(x)$ の根ならば，

$$0=f(\alpha)=a\cdot(\alpha-\alpha_1)(\alpha-\alpha_2)\cdots(\alpha-\alpha_n)$$

で，ある i に対して $\alpha=\alpha_i$ となる．したがって，$f(x)$ は (重複を数えて) K の中にきっちり n 個の根をもつ．

k に $f(x)$ のすべての根 $\alpha_1, \alpha_2, \cdots, \alpha_n$ を添加して

$$k(\alpha_1, \alpha_2, \cdots, \alpha_n)$$

をつくれば，この体は (K の中で) $f(x)$ が 1 次式の積に分解されるような k の最小の拡大体である．$k(\alpha_1, \alpha_2, \cdots, \alpha_n)$ を $f(x)$ の k 上の(最小)**分解体**とよぶ．

例 1　$f(x)=x^2-2$ は $\boldsymbol{Q}$ 上の多項式で，$\boldsymbol{Q}$ の拡大体 $\boldsymbol{R}$ に根 $\pm\sqrt{2}$ をもつ．したがって，$f(x)$ の $\boldsymbol{Q}$ 上の分解体は

$$\boldsymbol{Q}(\sqrt{2}, -\sqrt{2})= \boldsymbol{Q}(\sqrt{2})$$

である．

$f(x)=x^2+1$ は $\boldsymbol{R}$ の上の多項式で，$\boldsymbol{R}$ の拡大体 $\boldsymbol{C}$ に根 $\pm i$ をもつ．$f(x)$ の

$\boldsymbol{R}$ 上の分解体は

$$\boldsymbol{R}(i, -i)=\boldsymbol{R}(i)=\boldsymbol{C}.$$

しかし，一般には，$f(x)\in k[x]$ の1つの根 α を k に添加しても，これがただちに $f(x)$ の分解体になる訳ではない (次の例2参照).

例 2　$f(x)=x^3-2$ は $\boldsymbol{Q}$ の上の既約多項式で (2.6節例14)，$\boldsymbol{R}$ に1つの根 $\sqrt[3]{2}$ をもつ．$\boldsymbol{Q}$ に $\sqrt[3]{2}$ を添加した体 $\boldsymbol{Q}(\sqrt[3]{2})$ の上では

$$f(x)=(x-\sqrt[3]{2})(x^2+\sqrt[3]{2}x+(\sqrt[3]{2})^2)$$

と分解されるが，まだ1次式の積にはかけていない．ここで $x^2+\sqrt[3]{2}x+(\sqrt[3]{2})^2$ は虚根をもち，$\boldsymbol{Q}(\sqrt[3]{2})$ の上ではまだ既約多項式である (2.6節例11).

$x^2+\sqrt[3]{2}x+(\sqrt[3]{2})^2$ の根は

$$x=\frac{-\sqrt[3]{2}\pm\sqrt[3]{2}\cdot\sqrt{3}i}{2}=\sqrt[3]{2}\omega,\ \sqrt[3]{2}\omega^2$$

で，ω は $\dfrac{-1+\sqrt{3}i}{2}$ をあらわす．したがって，$\boldsymbol{Q}(\sqrt[3]{2})$ に ω を添加すれば $\boldsymbol{Q}(\sqrt[3]{2})(\omega)=\boldsymbol{Q}(\sqrt[3]{2}, \omega)$ は $\sqrt[3]{2}\omega$ も $\sqrt[3]{2}\omega^2$ も含み，$f(x)$ の3つの根すべてを含む.

逆に，$\omega=\dfrac{\sqrt[3]{2}\omega}{\sqrt[3]{2}}$ とみれば $\boldsymbol{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)$ は $\boldsymbol{Q}(\sqrt[3]{2}, \omega)$ を含み

$$\boldsymbol{Q}(\sqrt[3]{2}, \omega)=\boldsymbol{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)$$

となって，これが $f(x)$ の $\boldsymbol{Q}$ 上の分解体であることが分かる.

$[\boldsymbol{Q}(\sqrt[3]{2}):\boldsymbol{Q}]=3$，$[\boldsymbol{Q}(\omega):\boldsymbol{Q}]=2$ から，$f(x)$ の分解体の $\boldsymbol{Q}$ 上の次数は $[\boldsymbol{Q}(\sqrt[3]{2}):\boldsymbol{Q}]\cdot[\boldsymbol{Q}(\omega):\boldsymbol{Q}]=6$ である (演習問題23).

例 3　$f(x)=(x^2-2)(x^2-3)$ は $\boldsymbol{Q}$ 上の多項式である．x^2-2 は $\boldsymbol{Q}$ 上で既約で，$\boldsymbol{Q}$ の拡大体 $K_1=\boldsymbol{Q}[x]/(x^2-2)$ に根 α_1 をもつ．α_1 を $\sqrt{2}$ としてよい (4.2節例8).

$$K_1=\boldsymbol{Q}(\sqrt{2})=\{a+b\sqrt{2}\mid a, b\in\boldsymbol{Q}\}.$$

K_1 では $f(x)$ は

$$f(x)=(x-\sqrt{2})(x+\sqrt{2})(x^2-3)$$

と分解されるが，完全に1次式の積ではない.

実際，x^2-3 は K_1 で既約である．もし x^2-3 が K_1 に根 $a+b\sqrt{2}$ をもつならば，

$$(a+b\sqrt{2})^2-3=0, \quad (a^2+2b^2-3)+2ab\sqrt{2}=0.$$

$ab\neq 0$ ならば $\sqrt{2}$ は有理数になって矛盾を生ずる．したがって

$$ab=0, \quad a^2+2b^2-3=0.$$

ここで $a=0$ ならば $b^2=\dfrac{3}{2}$，$b=0$ ならば $a^2=3$ で，いずれも矛盾である．

$f(x)$ を 1 次式の積に分解するには，K_1 を更に拡大する必要がある．x^2-3 は K_1 の拡大体 $K_2=K_1[x]/(x^2-3)$ に根 β をもつ．β を $\sqrt{3}$ としてよい．

$$K_2=\{(a+b\sqrt{2})+(c+d\sqrt{2})\sqrt{3} \mid a, b, c, d \in \boldsymbol{Q}\}.$$

この K_2 はちょうど $\boldsymbol{Q}(\sqrt{2}, \sqrt{3})$ に等しい (4.3 節例 4)．ここでは

$$f(x)=(x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{3})(x+\sqrt{3})$$

と 1 次式の積に分解される．$\boldsymbol{Q}(\sqrt{2}, \sqrt{3})$ が $f(x)$ の $\boldsymbol{Q}$ 上の分解体である．この分解体の $\boldsymbol{Q}$ 上の次数は 4 である (4.3 節例 2)．

k を体，$f(x)$ を k 上の n 次の多項式とする．$f(x)$ が k の適当な拡大体 K に根 $\alpha_1, \alpha_2, \cdots, \alpha_n$ をもつとして，$f(x)$ の k 上の分解体

$$k(\alpha_1, \alpha_2, \cdots, \alpha_n)$$

をつくる．k の他の拡大体 K' に $f(x)$ の根 $\alpha_1', \alpha_2', \cdots, \alpha_n'$ があれば，

$$k(\alpha_1', \alpha_2', \cdots, \alpha_n')$$

もまた $f(x)$ の k 上の分解体である．しかし，この 2 つの分解体は実は環同型である．以下このことを証明する．

4.2 節の最後にのべたように，体 $k, \bar{k}$ と環同型 $\varphi: k \to \bar{k}$ に対して写像 φ_1 を

$$\varphi_1: k[x] \to \bar{k}[x], \quad g(x)=\sum a_i x^i \to \bar{g}(x)=\sum \varphi(a_i) x^i$$

ときめると，φ_1 は環同型であって図 4.3 の図型は可換となった．

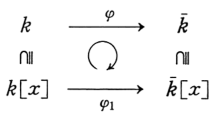


図 4.3

φ_1 の定義から $\bar{g}(x)$ の次数は $g(x)$ の次数と等しく，

$$g(x) \text{ が既約} \Leftrightarrow \bar{g}(x) \text{ が既約}$$

でもあった．

この記号を用いて次の定理を証明する．

定理 4.13 $k, \bar{k}$ は体で，$\varphi: k \to \bar{k}$ は環同型とする．$f(x) \in k[x]$ を n ($\geqq 1$) 次の多項式とすると，φ は $f(x)$ の k 上の分解体 $K=k(\alpha_1, \alpha_2, \cdots, \alpha_n)$ から $\bar{f}(x)$ の $\bar{k}$ 上の分解体 $\bar{K}=\bar{k}(\bar{\alpha}_1, \bar{\alpha}_2, \cdots, \bar{\alpha}_n)$ への環同型

$$\varphi_0: K \to \bar{K}$$

に拡張されて

$$\varphi_0(\alpha_i)=\bar{\alpha}_i \qquad (1\leqq i\leqq n)$$

が成り立つ(図 4.4).

$$\begin{array}{ccc} k & \xrightarrow{\ \varphi\ } & \bar{k} \\ \cap\!\| & \circlearrowright & \cap\!\| \\ K & \xrightarrow[\ \varphi_0\ ]{} & \bar{K} \end{array}$$

図 4.4

証明　定理 4.9 から K は k の有限拡大であるから $[K:k]$ は有限である．この $[K:k]$ に関する帰納法で証明する．

$[K:k]=1$ のときは，$\alpha_1, \alpha_2, \cdots, \alpha_n$ のすべてが k に属し，$f(x)$ は k で 1 次式の積に分解される．

$$f(x)=a\cdot(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) \qquad (a, \alpha_1, \alpha_2, \cdots, \alpha_n\in k).$$

この両辺に φ_1 を施すと，$\bar{f}(x)$ は

$$\bar{f}(x)=\varphi(a)\cdot(x-\varphi(\alpha_1))\cdots(x-\varphi(\alpha_n)) \qquad (\varphi(a), \varphi(\alpha_1), \cdots, \varphi(\alpha_n)\in\bar{k})$$

のように 1 次式の積に分解される．

$\bar{K}$ に属する $\bar{f}(x)$ の根 $\bar{\alpha}_i$ に対して

$$0=\bar{f}(\bar{\alpha}_i)=\varphi(a)\cdot(\bar{\alpha}_i-\varphi(\alpha_1))\cdots(\bar{\alpha}_i-\varphi(\alpha_n))$$

となるから，$\bar{\alpha}_i$ は $\varphi(\alpha_1), \varphi(\alpha_2), \cdots, \varphi(\alpha_n)$ のいずれかと一致し，したがって，$\bar{k}$ に属し，$\bar{K}=\bar{k}(\bar{\alpha}_1, \bar{\alpha}_2, \cdots, \bar{\alpha}_n)=\bar{k}$ となる．このとき定理は明らかである．

$[K:k]>1$ とし，$[K:k]$ より低い次数の場合には定理は正しいものと仮定する．$f(x)$ を $k[x]$ で既約多項式の積 $p_1(x)p_2(x)\cdots p_s(x)$ に分解する．ここで次数が 2 以上の既約多項式がある．その 1 つを $p_1(x)$ とし，簡単にこれを $p(x)$ とかく．$p(x)$ は $\alpha_1, \alpha_2, \cdots, \alpha_n$ のいずれかを根にもつ．

実際，各 $p_i(x)$ を $K[x]$ で既約多項式の積に分解すれば，$f(x)$ の $K[x]$ における既約多項式の積への分解がえられ，それは一方では $x-\alpha_1, x-\alpha_2, \cdots, x-\alpha_n$ の積に等しいはずである．素元分解の一意性から，$p(x)$ はいくつかの $x-\alpha_i$ の積でかける．したがって，$p(x)$ はいずれかの α_i を根にもつ．

そこで α_1 が $p(x)$ の K における 1 つの根とする．同じようなことが $\bar{p}(x)$ でも成り立つから，$\bar{\alpha}_1$ が $\bar{p}(x)$ の $\bar{K}$ における 1 つの根とする．

補題 4.6 から φ は環同型

$$\varphi_2\colon k(\alpha_1)\rightarrow\bar{k}(\bar{\alpha}_1)$$

に拡張されて，$\varphi_2(\alpha_1)=\bar{\alpha}_1$ が成り立つ．

$k(\alpha_1)[x], \bar{k}(\bar{\alpha}_1)[x]$ では，それぞれ

$$f(x)=(x-\alpha_1)f_1(x), \quad \bar{f}(x)=(x-\bar{\alpha}_1)\bar{f}_1(x)$$

と分解され，$f_1(x)$ の $k(\alpha_1)$ 上の分解体は $k(\alpha_1)(\alpha_2, \cdots, \alpha_n)=k(\alpha_1, \alpha_2, \cdots, \alpha_n)=K$，$\bar{f}_1(x)$ の $\bar{k}(\bar{\alpha}_1)$ 上の分解体は $\bar{k}(\bar{\alpha}_1)(\bar{\alpha}_2, \cdots, \bar{\alpha}_n)=\bar{K}$ である．

帰納法の仮定で，φ_2 は環同型

$$\varphi_3: K \to \bar{K}$$

に拡張されて $\varphi_3(\alpha_i)=\bar{\alpha}_i\ (2 \leqq i \leqq n)$ が成り立つ．

$\varphi_3(\alpha_1)=\varphi_2(\alpha_1)=\bar{\alpha}_1$ でもあるから定理は証明された．

特に，k 上の多項式 $f(x)$ の 2 つの分解体は環同型である．

4.5 有 限 体

有限個の元からなる体を**有限体**とよぶ．

例 1 2.2 節例 9 でのべたように，p が素数ならば

$$\boldsymbol{Z}/(p)=\{\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{p-1}\} \qquad (\bar{i}=i+(p))$$

は p 個の元からなる有限体である．

Kを有限体とする．体Kの標数は 0 か素数である (2.3 節例 10) が，もし 0 ならば，Kは $\boldsymbol{Q}$ と環同型な素体を含み (定理 2.8)，Kが有限個の元しかもたないことに矛盾する．したがって，Kの標数は素数でなければならない．

定理 4.14 有限体Kの標数は素数である．これを p とかけば，Kの素体は $\boldsymbol{Z}/(p)$ と環同型である．

Kを有限体，k, p をKの素体，標数とする．Kを k 上のベクトル空間とみたとき，Kは有限個の元しかもたないから，k 上有限次元である．$[K:k]=n$ とおきKの k 上の基底を $\alpha_1, \alpha_2, \cdots, \alpha_n$ とかけば，Kは k-加群とみて

$$K=k\alpha_1 \oplus k\alpha_2 \oplus \cdots \oplus k\alpha_n \cong k^n$$

とあらわされる (定理 3.6, 3.7)．k の位数は $|\boldsymbol{Z}/(p)|=p$ であるから $|K|=p^n$ となる．

零元でないKの元の全体 K^* は乗法に関してアーベル群をつくる．その位数は p^n-1 であり，K^* の任意の元 α に対して定理 1.19 から

$$\alpha^{p^n-1}=1.$$

したがって，$\alpha^{p^n}=\alpha$ である．この式はKの零元によってもみたされるから，K

のすべての元が多項式

$$f(x)=x^{p^n}-x$$

の根である．$f(x)\in K[x]$ でその次数は p^n であるから，Kはちょうど$f(x)$の根の全体と一致している(定理2.15)．

$f(x)$ はKにおいて

$$f(x)=\prod_{\alpha\in K}(x-\alpha)$$

と分解される．

kにKの元すべてを添加したものはKに等しく，それはkに$f(x)$の根すべてを添加したものであるから$f(x)$ の k 上の分解体になっている．

定理 4.15　Kを有限体，k, pをKの素体，標数とする．Kはk の有限拡大でk 上の次数を n とおけば，Kの位数は

$$|K|=p^n$$

である．Kはk 上の多項式

$$f(x)=x^{p^n}-x$$

の根の全体と一致し，$f(x)$ の k 上の分解体でもある．

K, K' を有限体とし，k, k' と，p, p' をそれぞれの素体と標数とする．$k\cong\boldsymbol{Z}/(p)$ であり $k'\cong\boldsymbol{Z}/(p')$ である．

$|K|=p^n, |K'|=p'^{n'}$ とかき $|K|=|K'|$ とするならば，$p^n=p'^{n'}$ で素因数分解の一意性から $p=p', n=n'$ をうる．したがって，

$$k\cong\boldsymbol{Z}/(p)\cong k'$$

であり，また，K も K' も共に

$$f(x)=x^{p^n}-x$$

の分解体である．定理4.13から次の定理をうる．

定理 4.16　位数の等しい2つの有限体は環同型である．

例 2　有限体Kの位数はすべて p^n の形をしている．$n=1$ のときは，KはKの素体k と一致して

$$K\cong\boldsymbol{Z}/(p).$$

$n>1$ のときは，$f(x)$ を k 上の n 次の既約多項式とする．$f(x)$ は k の拡大体 $k[x]/(f(x))$ に1つの根 α をもち，$k[x]/(f(x))=k(\alpha)$ が成り立つ(定理4.5)．定理4.4によれば $[k(\alpha):k]=n$ で，したがって，$|k(\alpha)|=p^n$．Kと $k(\alpha)$ は同じ位数をもつから

$$K\cong k(\alpha).$$

このように，k 上の n 次の既約多項式が 1 つあれば，それによって位数 p^n の有限体がつくれる．有限体の位数はすべて p^n の形をしているから，任意の自然数 n に対して k 上の n 次の既約多項式が存在すれば，すべての有限体を構成することができる．この問題には後に触れる（定理 4.24）．

k 上の n 次の既約多項式は一般には 1 つとはかぎらない．例えば，$k=\boldsymbol{Z}/(2)$ の上で x^3+x+1 も x^3+x^2+1 も共に既約である．しかし，定理 4.16 はそれから構成される 2 つの有限体は環同型であることを示している．

例 3 位数が $2^3=8$ の有限体は，$k=\boldsymbol{Z}/(2)$ とし k 上の 3 次の既約多項式

$$f(x)=x^3+x+1$$

によって構成できる．

$f(x)$ は k の拡大体 $k[x]/(f(x))$ に 1 つの根 α をもち，$k[x]/(f(x))=k(\alpha)$ が成り立つ．$k(\alpha)$ は $2^3=8$ 個の元からなる有限体で，4.2 節例 7 に示したように $k(\alpha)=\{0, 1, \alpha, 1+\alpha, \alpha^2, 1+\alpha^2, \alpha+\alpha^2, 1+\alpha+\alpha^2\}$ である．

$\alpha^3+\alpha+1=0$ から $\alpha^3=1+\alpha$．したがって

$$\alpha^4=\alpha+\alpha^2, \alpha^5=\alpha^2+\alpha^3=1+\alpha+\alpha^2, \alpha^6=(1+\alpha)^2=1+\alpha^2,$$
$$k(\alpha)=\{0, 1, \alpha, \alpha^2, \cdots, \alpha^6\}$$

ともかける．

また，$\alpha^6=1+\alpha^2$ は α^2 も $f(x)$ の根であることを示している．その上

$$(\alpha^4)^3+\alpha^4+1=(\alpha^6)^2+\alpha^4+1=(1+\alpha^2)^2+\alpha^4+1=0$$

から，α^4 も $f(x)$ の根である．$k(\alpha)$ で

$$f(x)=(x-\alpha)(x-\alpha^2)(x-\alpha^4)$$

と 1 次式の積に分解される．

$$k(\alpha, \alpha^2, \alpha^4)=k(\alpha)$$

が成り立って，$k(\alpha)$ は $f(x)$ の k 上の分解体でもある．

位数が $2^3=8$ の有限体は $k=\boldsymbol{Z}/(2)$ の上の 3 次の既約多項式

$$f_1(x)=x^3+x^2+1$$

によっても構成できる．$f_1(x)$ は $k[x]/(f_1(x))$ に 1 つの根 β をもち，$k[x]/(f_1(x))=k(\beta)$ が求める位数 8 の有限体である．

$k(\alpha), k(\beta)$ は同じ位数の有限体であるから環同型である．k の元を動かさない環同型 φ: $k(\alpha)\to k(\beta)$ を具体的に求めてみよう．

α は $f(x)$ の根であるから $\alpha^3+\alpha+1=0$，したがって，φ を施して

$$\varphi(\alpha)^3+\varphi(\alpha)+\varphi(1)=\varphi(\alpha^3+\alpha+1)=0.$$

これから $\varphi(\alpha)$ は $f(x)=0$ をみたす $k(\beta)$ の元であることが分かる．このよう

な $k(\beta)$ の元として $\beta^3=\beta^2+1$，$\beta^6=\beta^2+\beta$，$\beta^{12}=\beta+1$ がある．

$\varphi(\alpha)=\beta^3$ ときめると $\varphi\colon k(\alpha)\to k(\beta)$ は

$$\varphi(a_0+a_1\alpha+a_2\alpha^2)=a_0+a_1\beta^3+a_2\beta^6=(a_0+a_1)+a_2\beta+(a_1+a_2)\beta^2$$

とあらわされる．この φ が環同型であることを確かめるのは演習問題とする．

$\varphi(\alpha)=\beta^6$ とおくなり，$\varphi(\alpha)=\beta^{12}$ とおいても同じように環同型がえられる．

Kが有限体ならば，素数 p と自然数 n があって，Kのすべての元は

$$f(x)=x^{p^n}-x$$

の根であった．逆に，素数 p と自然数 n を与えたとき，$f(x)=x^{p^n}-x$ の根の全体が位数 p^n の有限体をなすことを示す．

補題 4.17　k が標数 p の体，n が自然数ならば，k の任意の元 a, b に対して

$$(a\pm b)^{p^n}=a^{p^n}\pm b^{p^n}$$

が成り立つ．

証明　$n=1$ のときは，二項定理によって

$$(a+b)^p=\sum_{i=0}^{p}{}_p\mathrm{C}_i\,a^{p-i}b^i.$$

この証明は演習問題とする．ここで ${}_p\mathrm{C}_i$ は二項係数 $\dfrac{p!}{i!(p-i)!}$ を意味する．$1\leqq i\leqq p-1$ ならば，$p\,|\,{}_p\mathrm{C}_i$ (2.6 節) で，したがって，

$${}_p\mathrm{C}_i\,a^{p-i}b^i=0\qquad(1\leqq i\leqq p-1).$$

このことから $(a+b)^p=a^p+b^p$ をうる．$(a-b)^p$ に関しては

$$(a-b)^p=\sum_{i=0}^{p}(-1)^i{}_p\mathrm{C}_i\,a^{p-i}b^i$$

に注意すればよい．

$n>1$ のときは $(a+b)^{p^n}=a^{p^n}+b^{p^n}$ を仮定すれば，$(a+b)^{p^{n+1}}=(a^{p^n}+b^{p^n})^p=a^{p^{n+1}}+b^{p^{n+1}}$ と証明できる．

一般に，体 k の上の定数でない多項式 $f(x)$ に対して，α が $f(x)$ の根であることは $(x-\alpha)\,|\,f(x)$ を意味したが (補題 2.14)，ある自然数 m があって $f(x)$ が $(x-\alpha)^m$ で割り切れるが $(x-\alpha)^{m+1}$ では割り切れないとき，α を $f(x)$ の $\boldsymbol{m}$ **重根**とよぶ．$m\geqq 2$ のとき α を $f(x)$ の**重根**，$m=1$ のとき α を $f(x)$ の**単根**ともよぶ．

α が重根であるかどうかを判定するのに，多項式の微分という概念が有効である．多項式 $f(x)$ が

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$$

であるとき，$f(x)$ の**微分**を

$$f'(x)=a_1+2a_2x+\cdots+ia_ix^{i-1}+\cdots+na_nx^{n-1}$$

ときめる（演習問題37参照）．

k が標数 p の体，n が自然数のとき，k の上の多項式

$$f(x)=x^{p^n}-x$$

が k の拡大体 K で m 重根 α $(m>1)$ をもつならば，$K[x]$ で

$$x^{p^n}-x=(x-\alpha)^m\cdot g(x)$$

とかける．両辺の微分をとって

$$p^nx^{p^n-1}-1=m(x-\alpha)^{m-1}\cdot g(x)+(x-\alpha)^m\cdot g'(x).$$

x に α を代入すると左辺は -1，右辺は $m>1$ から 0 になって矛盾を生ずる．$f(x)$ は重根をもつことはない．$f(x)$ の相異なる根はちょうど p^n 個ある．

定理 4.18 k を標数 p の体，n を自然数とする．k の上の多項式

$$f(x)=x^{p^n}-x$$

の根の全体は位数 p^n の有限体をつくる．

証明 $f(x)$ の k 上の分解体を K とする．$f(x)$ は K に p^n 個の相異なる根をもつ．α,β が2つの根ならば

$$(\alpha-\beta)^{p^n}=\alpha^{p^n}-\beta^{p^n}=\alpha-\beta,$$

$$(\alpha\beta^{-1})^{p^n}=\alpha^{p^n}\cdot(\beta^{p^n})^{-1}=\alpha\beta^{-1}\quad(\beta\neq 0 \text{ のとき})$$

が成り立つから，p^n 個の根の全体は K の部分体をつくる（補題2.3）．

定理4.18は，任意の素数 p，自然数 n に対して，位数 p^n の有限体が既約多項式とは無関係に存在することを示している．定理4.15, 4.18から分かるように，多項式

$$f(x)=x^{p^n}-x$$

は有限体と深く関連している．この意味で，この多項式を有限体の**特性多項式**とよぶ．

位数が同じ有限体はすべて環同型であった．同型を除けば一意的にきまる位数 p^n の有限体を $GF(p^n)$ であらわし，位数 p^n の**ガロア体**ともよぶ．

定理 4.19 K を位数 p^n の有限体とする．K の任意の部分体の位数は p^m（m は n の正の約数）である．

逆に，m が n の正の約数ならば，位数 p^m の K の部分体がただ1つ存在する．

証明　Kを位数p^nの有限体，kをKの素体とする．$[K:k]=n$である．Kの部分体K'に対しても$k\subseteqq K'$であり，$[K':k]=m$とおけば$|K'|=p^m$であるが，$[K:k]=[K:K']\cdot[K':k]$であるからmはnの正の約数である．

逆の証明には次の補題を用いる．

補題 4.20　体k上の多項式x^m-1，x^n-1 (m,nは自然数) に対して

$$m|n \Leftrightarrow (x^m-1)\,|\,(x^n-1).$$

証明　$n=mq+r$ ($0\leqq r<m$) ときめる．

$$x^n-1=x^{mq}\cdot x^r-1$$

で，$x^{mq}-1=(x^m-1)(1+x^m+x^{2m}+\cdots+x^{(q-1)m})$であるから

$$\begin{aligned}x^n-1&=\{(x^m-1)(1+x^m+\cdots+x^{(q-1)m})+1\}\cdot x^r-1\\&=(x^m-1)(1+x^m+\cdots+x^{(q-1)m})\cdot x^r+x^r-1.\end{aligned}$$

ここで$r<m$であるから，上の式はx^n-1をx^m-1で割った剰余がx^r-1であることを示している．このとき$r=0 \Leftrightarrow x^r-1=0$であるから，$m|n$は$(x^m-1)|(x^n-1)$を示している．

なお，この証明はm,n,xを自然数としてもそのまま成り立つ．

定理4.19の逆の**証明**．補題4.20から

$$m|n \Leftrightarrow (p^m-1)|(p^n-1) \Leftrightarrow (x^{p^m-1}-1)|(x^{p^n-1}-1).$$

したがって，$m|n$ならばKの特性多項式$f(x)=x(x^{p^n-1}-1)$が$f_1(x)=x\cdot(x^{p^m-1}-1)$で割り切れる．$f_1(x)$の根はすべて$f(x)$の根で，$f_1(x)$の根の全体は位数$p^m$の$K$の部分体をつくる．

K'を上のように$f_1(x)$の根全体のつくるKの部分体とし，別に位数p^mのKの部分体K_1があったとする．K_1の元はすべて$f_1(x)$の根であるから$K_1\subseteqq K'$であり，2つの位数が等しいから一致する．

例 4　位数2^{30}の有限体$K=GF(2^{30})$の部分体は，30の正の約数をすべてあげることによって，図4.5のように与えられる．

一般に，0でない体の元の全体は乗法に関してアーベル群をつくるが，有限体のときはこれが巡回群であることを示す．

定理 4.21　有限体Kの乗法群K^*は巡回群である．

証明　Kの位数をp^nとおく．$p^n\geqq 3$としてよい．p^n-1の素因数分解を$p_1^{e_1}p_2^{e_2}\cdots p_m^{e_m}$ ($p_1,p_2,\cdots,p_m$は相異なる素数，$e_1,e_2,\cdots,e_m$は自然数) とする．各iに対して，多項式

$$x^{\frac{p^n-1}{p_i}}-1$$

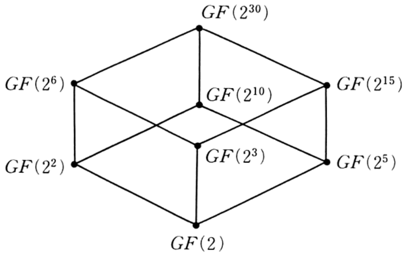


図 4.5

の K^* における根は高々 $\dfrac{p^n-1}{p_i}$ 個であり，$\dfrac{p^n-1}{p_i}<p^n-1$ であるから，K^* の中にはこの多項式の根ではない元 a_i が存在する．

$$b_i=a_i^{\frac{p^n-1}{p_i^{e_i}}}$$

ときめる．$b_i^{p_i^{e_i}}=a_i^{p^n-1}=1$ であるから b_i の位数は $p_i^{e_i}$ の約数であるが，$b_i^{p_i^{e_i-1}}=a_i^{\frac{p^n-1}{p_i}}\neq 1$ であるから，b_i の位数は $p_i^{e_i}$ に等しい．

このとき $b_1b_2\cdots b_m$ の位数は p^n-1 に一致する．実際，$(b_1b_2\cdots b_m)^{p^n-1}=1$ であるから，$b_1b_2\cdots b_m$ の位数は p^n-1 の約数であるが，もし p^n-1 の真の約数ならば，位数は

$$\frac{p^n-1}{p_1},\ \frac{p^n-1}{p_2},\ \cdots,\ \frac{p^n-1}{p_m}$$

のいずれかの約数でなければならない．簡単に $\dfrac{p^n-1}{p_1}$ の約数としよう．

$$1=(b_1b_2\cdots b_m)^{\frac{p^n-1}{p_1}}=b_1^{\frac{p^n-1}{p_1}}b_2^{\frac{p^n-1}{p_1}}\cdots b_m^{\frac{p^n-1}{p_1}}$$

において，$i\neq 1$ ならば $b_i^{\frac{p^n-1}{p_1}}=1$ であるから

$$1=b_1^{\frac{p^n-1}{p_1}}.$$

したがって，b_1 の位数は $\dfrac{p^n-1}{p_1}=p_1^{e_1-1}p_2^{e_2}\cdots p_m^{e_m}$ の約数となるが，これは b_1 の位数が $p_1^{e_1}$ であることに矛盾する．

K^* は位数 p^n-1 の元 $b_1b_2\cdots b_m$ をもつから巡回群である．

3.6 節例 8 によれば，有限アーベル群 K^* には最大位数 s をもつ元があり，

K^* の任意の元の位数は s の約数である．この事実から定理 4.21 を証明することもできるが，これは演習問題とする．

位数 p^n の有限体 K の乗法群 K^* は位数 p^n-1 の巡回群である．この生成元を K の**原始元**とよぶ．K は $\varphi(p^n-1)$ 個の原始元をもつ（定理 1.23）．その 1 つを α とすると

$$K=\{0, 1, \alpha, \alpha^2, \cdots, \alpha^{p^n-2}\}$$

であり，K の素体を k とかけば，

$$K=k(\alpha)$$

が成り立つ．素体にかぎらず次のようにのべることもできる．

定理 4.22　有限体 K の有限次拡大体は K の単純拡大で，その任意の原始元 α によって $K(\alpha)$ とあらわされる．

例 5　例 3 のように $k=GF(2)$ とし，k 上の既約多項式 $f(x)=x^3+x+1$ の 1 つの根 α を k に添加してえられる 8 個の元からなる有限体

$$k(\alpha)=\{0, 1, \alpha, \alpha^2, \cdots, \alpha^6\}$$

をつくる．このとき，

$$\alpha^7=\alpha\cdot(1+\alpha^2)=\alpha+\alpha^3=1$$

でもあるから，α の位数は 7，α は $k(\alpha)$ の原始元である．$k(\alpha)^*$ は $\varphi(7)=6$ 個の原始元をもつ．α と共に $\alpha^2, \alpha^3, \cdots, \alpha^6$ の 5 個の元がすべて位数 7 で，したがって，$k(\alpha)$ の原始元である．

例 6　例 5 に示したように，位数 p^n の有限体 K を構成するには，K の原始元を 1 つみつけて，そのべきで K^* をあらわしておくとよい．

例えば，位数 3^2 の有限体を構成するのに，$k=GF(3)$ の上の 2 次の既約多項式 $f(x)=x^2+2x+2$（これが既約であることの証明は演習問題とする）の 1 つの根を α とする．$k(\alpha)$ は位数 3^2 の有限体である．

α は $f(x)$ の根であるから

$$\alpha^2+2\alpha+2=0, \quad \alpha^2=-2\alpha-2=\alpha+1.$$

これから

$$\alpha^3=\alpha(\alpha+1)=\alpha^2+\alpha=-\alpha-2=2\alpha+1,$$
$$\alpha^4=(\alpha+1)^2=\alpha^2+2\alpha+1=-1=2,$$
$$\cdots \qquad \cdots$$

と計算していくと

$$\alpha^8=2^2=4=1$$

となって，α が $k(\alpha)$ の原始元であることが分かる．したがって，

$$k(\alpha)=\{0,1,\alpha,\alpha^2,\cdots,\alpha^7\}.$$

上の計算を表にまとめると表 4.1 のようになる．

表 4.1

$\alpha^0=1$	$\alpha^4=2$
$\alpha^1=\quad\alpha$	$\alpha^5=\quad 2\alpha$
$\alpha^2=1+\alpha$	$\alpha^6=2+2\alpha=2\cdot\alpha^2$
$\alpha^3=1+2\alpha$	$\alpha^7=2+\alpha=2\cdot\alpha^3$

表 4.1 から右の欄の元は左のものの 2 倍になっていることも分かる．$k(\alpha)$ の加法には α の 1 次式を，$k(\alpha)$ の乗法には α のべきを用いて計算するとよい．例えば，$\alpha^3\cdot\alpha^5=\alpha^8=1$ から $(\alpha^3)^{-1}=\alpha^5$ であることがただちに分かる (4.2 節例 7 参照)．

根 α が原始元であるような既約多項式を**原始既約多項式**とよぶことがある．その例をいくつかあげておく．

表 4.2

$GF(2)$ 上の原始既約多項式	x^2+x+1 x^3+x+1 x^4+x+1 x^5+x^2+1
$GF(3)$ 上の原始既約多項式	x^2+2x+2 x^3+2x+1 x^4+2x+2 x^5+2x+1

位数 p^n の有限体は，m が n の正の約数であるとき，またこのときにかぎって，位数 p^m の部分体をもった．この部分体の原始元は次の定理で与えられる．

定理 4.23 位数 p^n の有限体 K の原始元を α，m を n の正の約数とするとき，$s=\dfrac{p^n-1}{p^m-1}$ に対して，α^s は位数 p^m の K の部分体の原始元である．

証明 演習問題 1 の 41 から α^s の位数は $\dfrac{p^n-1}{(p^n-1,s)}=p^m-1$．したがって，$\{0,1,\alpha^s,(\alpha^s)^2,\cdots,(\alpha^s)^{p^m-2}\}$ は K の上の多項式 $f(x)=x^{p^m}-x$ の K における根の全体と一致し，位数 p^m の K の部分体をつくる．

定理 4.24 任意の有限体 K と自然数 m に対して，K 上の m 次の既約多項式

が存在する．

証明　$|K|=p^n$ とし，位数 $(p^n)^m$ の K の拡大体は原始元 α によって $K(\alpha)$ とかける．このとき $[K(\alpha):K]=m$ である．α は K 上代数的で，その K 上の最小多項式は m 次の既約多項式である．

定理 4.25　K が位数 p^n の有限体，$f(x)$ が K 上の m 次既約多項式ならば，$f(x)$ の根はすべて単根で，その1つを α とかけば

$$\alpha, \alpha^{p^n}, \alpha^{(p^n)^2}, \cdots, \alpha^{(p^n)^{m-1}}$$

が $f(x)$ の根の全体をつくす．

証明　$f(x)$ は K の拡大体 $K[x]/(f(x))$ に1つの根 α をもち，$K[x]/(f(x))=K(\alpha)$ が成り立つ．$[K(\alpha):K]=m$ であり，$|K(\alpha)|$ は $(p^n)^m$ に等しい．

α と共に $\alpha^{p^n}, \alpha^{(p^n)^2}, \cdots$ が $f(x)$ の根であることは補題4.17から分かる．これらの根がすべて異なることを示す．

ある i, j $(0\leqq i<j<m)$ に対して $\alpha^{(p^n)^i}=\alpha^{(p^n)^j}$ と仮定すると

$$\alpha^{(p^n)^{m-j+i}}=(\alpha^{(p^n)^i})^{(p^n)^{m-j}}=(\alpha^{(p^n)^j})^{(p^n)^{m-j}}=\alpha^{(p^n)^m}=\alpha.$$

$g(x)=x^{(p^n)^{m-j+i}}-x$ とおけば，$g(x)$ の K 上の分解体の中で $g(x)$ の根の全体 K_1 は位数 $(p^n)^{m-j+i}$ の部分体をつくる．$K(\alpha)\subseteqq K_1$ から定理4.19によって

$$mn|n(m-j+i), \quad m|(m-j+i).$$

しかし，$0<m-j+i<m$ であるからこれは矛盾である．

演 習 問 題 4

1.　K を体 k の拡大体とする．K の部分集合 S_1, S_2 に対して次のことを示せ．

(1)　$S_1\subseteqq S_2 \Rightarrow k(S_1)\subseteqq k(S_2)$.

(2)　$k(S_1)(S_2)=k(S_1\cup S_2)=k(S_2)(S_1)$.

2.　K を体 k の拡大体とする．K の部分集合 S に対して，S' を S の有限部分集合のすべてをわたらせてつくった $k(S')$ の和集合 $\cup_{S'}k(S')$ は．S を含む k と K の中間体であることを示せ，

3.　$p\,(>2)$ を素数とする．位数 p の有限体 k は $a^2=1$（1は k の単位元）をみたす元 a をきっちり2個もつことを示せ．

4.　K を体 k の拡大体，$\alpha\in K$ を k 上代数的とする．写像 $h: k[x]\to K$, $g(x)\to g(\alpha)$ に対して $\mathrm{Ker}\, h=(p(x))$ をみたす $p(x)$ $(\neq 0)$ は定数多項式ではありえないことを示せ．

5.　$\alpha=\sqrt{2}+i$ を根にもつ $\boldsymbol{Q}$ 上の3次の多項式は存在しないことを示せ．

6. Kを体kの拡大体，$\alpha\in K$をk上代数的とする．$f(x)\in k[x]$がモニックで$f(\alpha)=0$であるとき，次のことを示せ．

$$f(x)\text{ が }\alpha\text{ の }k\text{ 上の最小多項式} \Leftrightarrow f(x)\text{ は }k[x]\text{ で既約.}$$

7. $\boldsymbol{Q}(\sqrt{2},\sqrt{3})=\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\mid a,b,c,d\in\boldsymbol{Q}\}$を示せ．

8. $\boldsymbol{Q}(\sqrt{2},\sqrt{3})=\boldsymbol{Q}(\sqrt{2}+\sqrt{3})$を示せ．また，$\sqrt{2}+\sqrt{3}$の$\boldsymbol{Q}$上の最小多項式を求めよ．

9. $\boldsymbol{Q}(\sqrt{3},\sqrt{7})$，$\boldsymbol{Q}(\sqrt{3},i)$はいずれも単純拡大であることを示し，$\boldsymbol{Q}$上の次数を求めよ．

10. 複素数$\alpha=a+bi$ $(a,b\in\boldsymbol{R})$は$\boldsymbol{R}$上代数的である．$\boldsymbol{R}$上の最小多項式を求めよ．

11. $\alpha=1+\sqrt{2}+\sqrt{3}$の$\boldsymbol{Q}$上の最小多項式を求めよ．

12. $\sqrt{2}i$, $\sqrt[3]{2}i$の$\boldsymbol{Q}$上の最小多項式を求めよ．

13. $k=\boldsymbol{Z}/(3)$に対して$f(x)=x^2+x+2$は$k[x]$の既約多項式であることを示せ．また，体$k[x]/(f(x))$の乗積表をつくれ．

14. $k,\bar{k}$は体で$\varphi: k\to\bar{k}$は環同型とする．多項式環$k[x]$と$\bar{k}[x]$に対して写像φ_1を

$$\varphi_1: k[x]\to\bar{k}[x],\quad h(x)=\sum a_ix^i\to\bar{h}(x)=\sum\varphi(a_i)x^i$$

ときめる．次のことを示せ．

(1) φ_1は一意写像である．

(2) φ_1は全単射である．

(3) φ_1は環準同型である．

15. 前問で$h(x)\in k[x]$に対して，次のことを示せ．

$$h(x)\text{ が既約} \Leftrightarrow \bar{h}(x)\text{ が既約.}$$

16. $a=1+\sqrt{2}+\sqrt{3}$に対して$\dfrac{1}{\alpha+1}$を$\boldsymbol{Q}(\alpha)$の$\boldsymbol{Q}$上の基底であらわせ．

17. $\boldsymbol{Q}(\sqrt{2}+i)$の$\boldsymbol{Q}$上の基底を求めよ．

18. Kを体kの有限次拡大体，K'をkとKの中間体とするとき，次のことを示せ．

(1) $[K:k]=[K':k]\Rightarrow K=K'$.

(2) $[K:K']=[K:k]\Rightarrow K'=k$.

19. Kを体kの有限次拡大体とする．$[K:k]$が素数ならば，Kはkの単純拡大であることを示せ．

20. Kを体kの有限次拡大体とする．$f(x)\in k[x]$が既約で，その次数が

$[K:k]$ と互いに素ならば，$f(x)$ のKに属する根は k にすでに属することを示せ．

21.　Kを体 k の有限次拡大体とする．$\alpha \in K$ が k 上代数的で k 上の次数が n ならば，$k(\alpha)$ の各元の位数は n の約数であることを示せ．

22.　Kを体 k の拡大体とし，Kの部分体 K', K'' が k の有限拡大で $[K':k]$, $[K'':k]$ が互いに素ならば，$K \cap K'' = k$ を示せ．

23.　K を体 k の拡大体，α, β ($\in K$) を k 上代数的とする．$[k(\alpha):k]$, $[k(\beta):k]$ が互いに素ならば，次のことを示せ．

$$[k(\alpha, \beta):k] = [k(\alpha):k] \cdot [k(\beta):k].$$

24.　超越拡大は無限拡大であるが，逆は正しくないことを示せ．

25.　体 k の上の定数でない多項式 $f(x)$ が k に少なくとも 1 個の根をもてば，$f(x)$ は $k[x]$ で 1 次式の積としてあらわされることを示せ．

26.　体 k に関して次の二つは同値であることを示せ．

(1)　k の代数的拡大は k にかぎられる．

(2)　k は任意の拡大体において代数的に閉じている．

27.　Kが体 k の拡大体であるとき，次のことを示せ．

Kが k の代数的拡大 $\Leftrightarrow$ k を含むKの部分環は体．

28.　k が体，$f(x) \in k[x]$ で次数が n のとき，$f(x)$ の k 上の分解体がKならば次の式が成り立つことを示せ．

$$[K:k] \leqq n!.$$

29.　x^4+1 は $\boldsymbol{Q}$ で既約であることを示せ．また，$\boldsymbol{Q}$ 上の分解体を求め，$\boldsymbol{Q}$ 上の次数を求めよ．

30.　素数 p に対して，x^p-1 の $\boldsymbol{Q}$ 上の分解体を求めよ．また，$\boldsymbol{Q}$ 上の次数を求めよ．

31.　$k = \boldsymbol{Z}/(2)$ のとき，$f(x) = x^3+x^2+1$ は $k[x]/(f(x))$ で 1 次式の積に分解できることを示せ．

32.　Kは有限体，$|K| = p^n > 2$ とする．次のことを示せ．

(1)　Kのすべての元の和は 0 に等しい．

(2)　K^* のすべての元の積は -1 に等しい．

33.　Kを位数 p^n の有限体，$f(x)$ をK上の m 次既約多項式，α を $f(x)$ の一つの根とすると，$f(x)$ は $K(\alpha)$ の特性多項式 $x^{(p^n)^m}-x$ を割り切ることを示せ．

34.　有限体K上の既約多項式は重根をもたないことを示せ．

35.　Kが位数 p^n の有限体ならば，Kの特性多項式 $x^{p^n}-x$ は $k = GF(p)$ 上

の次数 m(m は n の正の約数) のすべてのモニックな既約多項式の積としてあらわされることを示せ.

36. $k=GF(2)$ として, x^4-x, x^8-x を前問の意味の既約多項式の積であらわせ.

37. 可換環 R の上の多項式 $f(x)=a_0+a_1x+\cdots+a_nx^n$ に対して

$$f'(x)=a_1+2a_2x+\cdots+na_nx^{n-1}$$

を $f(x)$ の**微分**とよぶ. $f'(x)$ を $(f(x))'$ ともかく. $f(x), g(x)\in R[x]$, $a\in R$ に対して, 次のことを示せ.

(1) $(f(x)+g(x))'=f'(x)+g'(x)$.

(2) $(a\cdot f(x))'=a\cdot f'(x)$.

(3) $(f(x)\cdot g(x))'=f'(x)\cdot g(x)+f(x)\cdot g'(x)$.

38. R が可換環ならば, $a, b\in R$ と $n>0$ に対して

$$(a+b)^n=\sum_{i=0}^{n}{}_n\mathrm{C}_i\,a^{n-i}b^i$$

であることを示せ. これを**二項定理**とよんでいる.

39. 位数 11 の有限体の原始元を 1 つ求めよ.

40. $k=GF(2)$ 上で x^3+x^2+1 は既約であることを示せ.

41. $k=GF(2)$ 上で x^4+x^3+1 は既約であることを示せ.

42. $k=GF(3)$ 上で x^2+2x+2 は既約であることを示せ.

43. $k=GF(3)$ 上で x^2+1 は既約であることを示せ. このとき, $k[x]/(x^2+1)$ は $3^2=9$ 個の元からなる有限体である. この体の原始元を 1 つ求めよ. また, 他の元をこの原始元であらわせ.

44. $k=GF(2)$ 上で $f(x)=x^3+x+1$ は既約であることを示し, 体 $k[x]/(f(x))$ の乗積表をつくれ.

45. $k=GF(3)$ の上で $f(x)=x^4+2x+2$ が既約であることを示せ. このとき, $f(x)$ は体 $k[x]/(f(x))$ に根 α をもつ. $k[x]/(f(x))$ の中で $2\alpha^3+2\alpha^2+1$ の乗法に関する逆元を求めよ.

46. k が標数 p の体, n が自然数ならば, 写像

$$f: k\to k, \quad a\to a^{p^n}$$

は k の自己同型であることを示せ.

47. $k=GF(2)$ として k 上の既約多項式 $f(x)=x^3+x+1$ の根 α を k に添加した $k(\alpha)$ と, k 上の既約多項式 $f_1(x)=x^3+x^2+1$ の根 β を k に添加した $k(\beta)$ を考える.

$$\varphi_0(a_0+a_1\alpha+a_2\alpha^2)=(a_0+a_1)+a_2\beta+(a_1+a_2)\beta^2$$

ときめると，φ_0: $k(\alpha) \to k(\beta)$ は環同型であることを示せ．

48. $k=GF(2)$ の上で $f(x)=x^2+1$ も $f_1(x)=x^2+2x+2$ も共に既約な多項式である．$f(x)$ の根 α, $f_1(x)$ の根 β をそれぞれ k に添加した $k(\alpha), k(\beta)$ に対して，写像 φ_0, ψ_0 で

$$\varphi_0, \psi_0 \colon k(\alpha) \to k(\beta) \qquad (\varphi_0(\alpha)=1+\beta, \psi_0(\alpha)=2+2\beta)$$

をみたす環同型があることを確かめよ．

49. 体 K の乗法群 K^* の有限部分群は巡回群であることを示せ．

50. K が体，K^* が巡回群ならば，K は有限体であることを示せ．

演習問題略解

演習問題 1

1. aをGの任意の元，eをGの右単位元，a'をaの右逆元，a''をa'の右逆元とする．このとき$ea''=(aa')a''=a(a'a'')=ae=a$．したがって，$ea=e(ea'')=(ee)a''=ea''=a$．これは$e$がGの単位元であることを示している．$(aa')a''=ea''=a''$であり，また$(aa')a''=a(a'a'')=ae=a$でもあるから$a=a''$．したがって，$a'a=a'a''=e$で$a'$は$a$の逆元である．

2. Z^*は空でなく，乗法に関して結合法則，左右の簡約律をみたすが，乗法に関して群をつくらない．

3. $a, b\in G$に対して，$a^2=e$から$a=a^{-1}$，同じように$b=b^{-1}$．$e=(ab)^2=aba^{-1}b^{-1}$で，$ba=ab$をうる．

4. $S_2=\left\{e=\begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix},\ a=\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}\right\}$．乗積表は右の通り．

	e	a
e	e	a
a	a	e

5. 単位元$(1,0)$，$(a,b)^{-1}=\left(\dfrac{1}{a}, -\dfrac{b}{a}\right)$．

$(0,1)\cdot(1,1)=(0,2), (1,1)\cdot(0,1)=(0,1)$からアーベル群ではない．

6. 単位元はϕ，$A^{-1}=A$．結合法則は図をかいてみると分かりやすい(図1)．

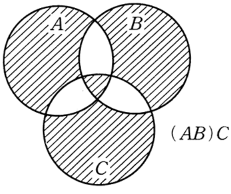


図 1

7. (2) 単位元は恒等写像，f^{-1}は$z\to\dfrac{dz-b}{-cz+a}$．

8. x軸，y軸，原点に関する対称移動は平面αの運動で，恒等写像とあわせて定理1.6の条件をみたす．

9. 正方形の重心のまわりの90°の回転をaとかく．恒等写像e, a, a^2, a^3と，直線l_1, l_2, l_3, l_4に関する対称移動b_1, b_2, b_3, b_4のあわせて8個の元が，平面αの運動で正方形をそれ自身に重ねるものの全体である．乗積表をつくって定理1.6の条件をみたすことを確かめよ．これら8個の運動を頂点の間の置換とみれば，

$$e=\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 3 & 4\end{pmatrix},\ a=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 4 & 1\end{pmatrix},\ a^2=\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 4 & 1 & 2\end{pmatrix},\ a^3=\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 1 & 2 & 3\end{pmatrix},$$

$$b_1=\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix},\ b_2=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},\ b_3=\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix},\ b_4=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$$

となる．$b_2=ab_1, b_3=a^2b_1, b_4=a^3b_1$ であるから，この群は a と b_1 の 2 元から生成される．

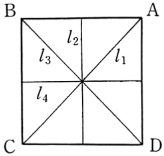


図 2

11.　n に関する帰納法．$n=3$ のときは結合法則．$n>3$ とし $n-1$ のときは正しいものと仮定すると $(a_1\cdots a_i)(a_{i+1}\cdots a_n)=(a_1\cdots a_i)(a_{i+1}\cdots a_{n-1}\cdot a_n)=((a_1\cdots a_i)(a_{i+1}\cdots a_{n-1}))\cdot a_n=a_1\cdots a_{n-1}\cdot a_n=a_1a_2\cdots a_n$.

12.　S の元の積の全体を H とおき，定理 1.6 を適用せよ．

13.　G の演算を φ とかく．H は φ で群をつくるから $H\times H\xrightarrow{\varphi}H$ は一意写像．特に $\varphi(a,b)=ab$ (G における積) とかけば，(1)　$a,b\in H\Rightarrow ab\in H$.　H は単位元 e_H をもつ．G で G の単位元 e との積をつくれば $e_H\cdot e=e_H=e_H\cdot e_H$. G における左簡約律から，(2)　$e=e_H\in H$.　$a\in H$ をとる．逆元 a' が H にある．a を G の元とみれば G における逆元 a^{-1} が G にある．$aa^{-1}=e=e_H=aa'$. G における左簡約律から　(3)　$a^{-1}=a'\in H$.

14.　群 G の部分群とは，G の演算で群をつくる G の部分集合であることに注意．

15.　(1)　$D_3=S_3$ であるから 1.1 節例 6 の記号を用いると，部分群は $\{e\},\{e,u\},\{e,v\},\{e,w\},\{e,a,a^2\},D_3$.　(2)　自明でない部分群は位数 2 のもの 5 個，位数 4 のもの 3 個．

16.　(2)　SS' が部分群ならば，S,S' の任意の元 s,s' に対して $s's=es'\cdot se\in SS'\cdot SS'=SS'$. したがって，$S'S\subseteqq SS'$. 逆も同じ．逆に，$SS'=S'S$ とする．$SS'\cdot SS'=S(S'S)S'=S(SS')S'=(SS)(S'S')=SS'$ で SS' は積で閉じる．S,S' の任意の元 s,s' に対して $(ss')^{-1}=s'^{-1}s^{-1}\in S'S=SS'$. SS' が単位元を含むことは明らか．

17.　G の任意の元 a に対して $a^{-1}\in K_i$ なる i がある．このとき $a=(a^{-1})^{-1}\in K_i^{-1}$.

18.　(5)　定理 1.10 を適用．

19.　(1)　$a\in H$, $b\in K$ ならば $ab=b(b^{-1}ab)\in KH$.

21.　(2)　$(G:H),(H:K)$ 共に有限とする．G の H を，H の K を法とする左剰余類の全体をそれぞれ $a_1H,\cdots,a_mH\ (a_i\in G), b_1K,\cdots,b_nK\ (b_j\in H)$ とする．このとき $(i,j)\neq(l,m)$ ならば $a_ib_jK\neq a_lb_mK$. もし $a_ib_jK=a_lb_mK$ ならば，$i\neq l$ のときは $a_ib_j=a_lb_mc$ なる $c\in K$ があり，$a_iH\cap a_lH\neq\phi$ で矛盾．$i=l, j\neq m$ のときは $a_ib_j=a_ib_mc$ から $b_j=b_mc, b_jK\cap b_mK\neq\phi$ で矛盾．　G の任意の元 a に対して $a\in a_iH$ なる i があり，$a=a_id\ (d\in H)$ とかく．$d\in b_jK$ なる j があり $a\in a_ib_jK$. $aK\cap a_ib_jK\neq\phi$. したがって，$aK=a_ib_jK$. このことは $(G:K)\leqq(G:H)\cdot(H:K)$ を意味する．特に $(G:K)$ は有限である．逆に，$(G:K)$ が有限とする．$a_1K,\cdots,a_mK$ を G の K を法とする左剰余類の全体とする．G の任意の元 a に対し $a\in a_iK\subseteqq a_iH$ なる i があり $aH=a_iH$. したがって，$(G:H)\leqq(G:K)$. 同じように $(H:K)\leqq(G:K)$. $(G:H),(H:K)$ は共に有限である．

25. (2) $f_af_b=f_{ab}, (f_a)^{-1}=f_{a^{-1}}, f_e=1_G$. $f\in A(G)$ ならば $ff_af^{-1}=f_{f(a)}$ を確かめよ.

26. (2) f を全射とする. 任意の素数 p に対して $p=f(a)$ をみたす $a\in \boldsymbol{Z}$ がある. $f(1)\mid p$ から $f(1)=\pm 1$.

28. G の元 a に対して写像 $g_a: G\to G$ を $x\to ax$ ときめる. g_a は G の上の対称群に属し $a\to g_a$ は G からこの対称群への単射準同型である.

29. 写像 $G\to G'/H'$, $a\to f(a)H'$ は一意, 全射準同型. 核は $\{a\in G\mid f(a)H=H\}=\{a\in G\mid f(a)\in H\}$.

30. 写像 $K\to KH/H$, $a\to aH$ は一意, 準同型. KH/H の任意の元 $abH\,(a\in K, b\in H)$ は $abH=aH\cdot bH=aH\cdot H=aH$ とかけるから全射でもある. 核は $\{a\in K\mid aH=H\}=\{a\in K\mid a\in H\}$.

31. (2) $N(a)$ を法とする左剰余類の全体から $K(a)$ への写像 $xN(a)\to xax^{-1}$ は一意かつ全単射.

32. (2) $x, a\in G$ に対して $\bigcap_{a\in G} aHa^{-1}\subseteqq xaH(xa)^{-1}$ から $x^{-1}(\bigcap aHa^{-1})x\subseteqq aHa^{-1}$. したがって, $x^{-1}(\bigcap aHa^{-1})x\subseteqq \bigcap aHa^{-1}$.

35. $m\mid(a-b)$ から $a-b=ms$ とかける. $b=a-ms$ で $(a,m)\mid b$. したがって, $(a,m)\mid(b,m)$.

37. $\boldsymbol{Q}^*\ni \dfrac{b}{a}>0$ とし $\left(\dfrac{b}{a}\right)^m=1$ とする. $a=1$ のとき $b=1$. $a>1$ のとき $b>1$ で, a, b を素因数分解して $a=p_1^{e_1}\cdots p_n^{e_n}, b=p_1^{f_1}\cdots p_n^{f_n}\ (e_i, f_i\geqq 0)$ とかけば $me_i=mf_i, e_i=f_i$. したがって, $a=b$.

38. $(ab)^m=e$ とすると $(ba)^{m+1}=b(ab)^ma=ba$. したがって, $(ba)^m=e$.

39. (1) ab の位数を l とおく. $(ab)^{mn}=a^{mn}b^{nm}=e$ から $l\mid mn$. また, $e=(ab)^{lm}=b^{lm}$ から $n\mid lm$. m, n が互いに素ならば $n\mid l$. 同じように $m\mid l$. $mn\mid l$ で $l=mn$. 逆に, $l=mn, (m,n)=d, m=dm', n=dn'$ とおく. $(ab)^{dm'n'}=e$ から $mn\mid dm'n'$. したがって $d=1$. (2) $(a)\cdot(b)$ の任意の元 a^ub^v に対して, $n\mid m$ ならば $(a^ub^v)^m=e$. a^ub^v の位数は m を割り切って m をこえることはない. 逆を示す. $m\neq 1, n\neq 1$ としてよい. $m=p_1^{e_1}\cdots p_n^{e_n}, n=p_1^{f_1}\cdots p_n^{f_n}$ を素因数分解とする. $n\nmid m$ ならば $e_i<f_i$ をみたす i がある. $i=1$ とする. $m=p_1^{e_1}m', n=p_1^{e_1+1}n'$ とかけば $a_1^{p_1^{e_1}}$ の位数は m', $b^{n'}$ の位数は $p_1^{e_1+1}$. したがって, $a^{p_1^{e_1}}b^{n'}$ の位数は $m'p_1^{e_1+1}=mp_1$ で m をこえて矛盾.

41. (2) $(a^n)^m=e$, $nm\neq 0$ から a^n の位数は無限ではない. a^n の位数を k とおく. $(a^n)^k=e$ から $m\mid nk$. $nk=mu$ とかけば $k\cdot\dfrac{n}{(m,n)}=u\cdot\dfrac{m}{(m,n)}$. $\dfrac{n}{(m,n)}$ と $\dfrac{m}{(m,n)}$ は互いに素から $\dfrac{m}{(m,n)}\Big| k$. また, $(a^n)^{m/(m,n)}=(a^m)^{n/(m,n)}=e$ から $k\Big|\dfrac{m}{(m,n)}$ で $k=\dfrac{m}{(m,n)}$ をうる.

43. (2) $G=(a)$, $G'=(a')$ が共に有限群で $|G|=m$, $|G'|=n$ とする. $n\mid m$ ならば $n\leqq m$ で $f: G\to G'$, $a^i\to a'^i$ は全射準同型. 逆に, $g: G\to G'$ が全射準同型ならば, $G/\mathrm{Ker}\, g\cong G'$ で $m=(G: \mathrm{Ker}\, g)\cdot|\mathrm{Ker}\, g|=n\cdot|\mathrm{Ker}\, g|$. $m=n$ とする. このとき g は単射となる. 実際, $a'^i=a'^j\,(i>j)$ ならば $a'^{i-j}=e'$, $m=n\mid(i-j)$ で $m=i-j$ となる. $e=a^m=a^{i-j}$ から $a^i=a^j$.

44.　$x\in G$，$x^s=e$ とする．$su+tv=1$ をみたす整数 u, v がある．$x=x^{su}\cdot x^{tv}=x^{tv}$．$(G:H)=t$ から $x^t\in H$．したがって，$x\in H$．

45.　(1)　$H_s=\{x\in G \mid x^s=1\}$ は位数 s の巡回群で，位数 s の G の元は H_s の生成元，その個数は $\varphi(s)$．

46.　$G=(a), G'=(a')$ とする．m, m' が互いに素ならば，$(a,e')\cdot(e,a')$ は $G\times G'$ の位数 mm' の元である．m, m' が互いに素でないとき，最小公倍数 l は mm' より小さく，$G\times G'$ の任意の元 (b,b') に対して $(b,b')^l=(e,e')$ をみたすから，$G\times G'$ は巡回群ではない．

47.　(2)　G が H, K の直積に分解されるとする．$ab\in G$, $a'\in H$ をとれば $ab\cdot a'\cdot(ab)^{-1}=aa'a^{-1}\in H$．$H\cap K\ni a=b$ をとる．$a\cdot e=e\cdot b\in HK$．一意性から $a=e$．逆に，$H, K\lhd G, G=HK, H\cap K=\{e\}$ とする．$a\in H, b\in K$ ならば，$aba^{-1}b^{-1}\in K\cap H=\{e\}$，したがって，$ab=ba$．$ab, a'b'\in G$ をとる．$ab=a'b'$ ならば，$a'^{-1}a=b'b^{-1}\in H\cap K$．したがって，$a=a', b=b'$．

48.　H を $\boldsymbol{Q}$ の部分群で $(\boldsymbol{Q}:H)=n$ とする．$\boldsymbol{Q}$ の任意の元 a に対して $\dfrac{a}{n}\in\boldsymbol{Q}$ であるから $a=n\cdot\dfrac{a}{n}\in H$．

50.　G が位数 p^2 の元を含まないときは，$G\ni a\neq e$ ならば (a) は位数 p の部分群．(a) に属さない G の元 b をとれば (b) も位数 p の部分群で $(a)\cap(b)=\{e\}$，$G=(a)(b)$ が成り立つ．

55.　$i, j\geqq 2\ (i\neq j)$ ならば $(i\ \ j)=(1\ \ i)(1\ \ j)(1\ \ i)$ であることによる．

56.　(1)　$\{e\}, \{(1\ \ 2), (1\ \ 3), (2\ \ 3)\}, \{(1\ \ 2\ \ 3), (1\ \ 3\ \ 2)\}$ の3つ．

57.　演習問題1の52(1)による．

60.　S_n の元を $(1\ \ a)$ の形の互換の積の形にあらわしておく．$f((1\ 2))^2=f((1\ 2)^2)=f(e)=1$ から $f((1\ \ 2))=\pm 1$．しかも $(1\ \ a)=(2\ \ a)(1\ \ 2)(2\ \ a)$ から $f((1\ \ a))=f((2\ \ a))^2\times f((1\ \ 2))=f((1\ \ 2))$．したがって，$f((1\ \ 2))=1$ のときは①が，$f((1\ \ 2))=-1$ のときは②となる．

演習問題 2

1.　演習問題1の6参照．

2.　(1)　R は零元をもたない．　(2)　R は積で閉じない．例えば，$\dfrac{1}{2}\cdot\dfrac{1}{2}=\dfrac{1}{4}$．
(3)　R は積で閉じない．例えば，$\begin{pmatrix}0&1\\0&0\end{pmatrix}\cdot\begin{pmatrix}0&0\\1&0\end{pmatrix}=\begin{pmatrix}1&0\\0&0\end{pmatrix}$．　(4)　R は加法に関して逆元をもたない．

3.　$f\in R$，$f\neq 0$ とする．すべての $x\in X$ に対して $f(x)\neq 0$ のときは f は単元で，そうでないときは f は零因子である．

9.　$a+bi$ が $\boldsymbol{Z}[i]$ の単元 $\Leftrightarrow$ $a=0, b=\pm 1$ または $a=\pm 1, b=0$．

11.　例えば，$\dfrac{1}{\sqrt{2}}$ は R に属さない．

15.　$R'\cup R''$ は部分環で，$R'\subsetneqq R''$, $R''\subsetneqq R'$ と仮定する．$a\in R', a\notin R''$，$b\in R''$，$b\notin R'$

なるRの元a, bがある．$a+b\in R'\cup R''$であり，$a+b\in R'$ならば$b=(-a)+(a+b)\in R'$で矛盾，$a+b\in R''$ならば同様に$a\in R''$で矛盾である． 逆は明らか．反例は$(\boldsymbol{R})_2$の部分環$\begin{pmatrix}\boldsymbol{R} & \boldsymbol{R}\\ 0 & \boldsymbol{R}\end{pmatrix}$と$\begin{pmatrix}\boldsymbol{R} & 0\\ \boldsymbol{R} & \boldsymbol{R}\end{pmatrix}$.

16. (2) $A=\{0,1\}$, $B=C=\{1\}$ならば$A\cdot(B+C)=\{0,2\}$, $AB+AC=\{0,1,2\}$.

18. $S=\{1,2,3\}$とかけば$R=\{\phi, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, S\}$．部分環は単位元$S$，零元$\phi$を含み，加法群$R$の部分群．したがって，その位数は$2,4,8$． 位数2の部分環は$\{\phi, S\}$．位数4の部分環が$\{1\}$を含めば$S+\{1\}=\{2,3\}$を含まなければならない．$\{\phi, S, \{1\}, \{2,3\}\}$は部分環．$\{\phi, S, \{2\}, \{1,3\}\}$, $\{\phi, S, \{3\}, \{1,2\}\}$も部分環． Rのイデアルは零元を含み，加法群Rの部分群．その位数は$1,2,4,8$．位数2のイデアルは$\{\phi, \{1\}\}$, $\{\phi, \{2\}\}$, $\{\phi, \{3\}\}$．$\{\phi, \{1,2\}\}$等はイデアルではない．位数4のイデアルは$\{\phi, \{1\}, \{2\}, \{1,2\}\}$等.

20. $a_{11}=0$で$a_{12}\neq 0$のときは$\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}\cdot\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$を求めて2.2節例6にならったらよい．$a_{21}\neq 0, a_{22}\neq 0$のときも同様.

21. (2) $(R)_2$のイデアルBに対して，あるi, jがあってaを(i,j)成分にもつ行列がBに属するようなRの元aの全体をAとおく．$A=\left\{a\in R \,\middle|\, \begin{pmatrix}a & 0\\ 0 & 0\end{pmatrix}\in B\right\}$としてもよい. AはRのイデアルで$B=(A)_2$が成り立つ.

22. $\begin{pmatrix}0 & \boldsymbol{R}\\ 0 & 0\end{pmatrix}, \begin{pmatrix}\boldsymbol{R} & \boldsymbol{R}\\ 0 & 0\end{pmatrix}, \begin{pmatrix}0 & \boldsymbol{R}\\ 0 & \boldsymbol{R}\end{pmatrix}$は確かに$R$のイデアルである．これ以外にイデアル$A$があったとする．$A\neq\{0\}$ならば，$A$の中に$\begin{pmatrix}a & b\\ 0 & c\end{pmatrix}$で$a\neq 0, c\neq 0$であるものがある．このとき$R$の任意の元$\begin{pmatrix}a' & b'\\ 0 & c'\end{pmatrix}$に対して

$$\begin{pmatrix}a' & b'\\ 0 & c'\end{pmatrix}=\begin{pmatrix}1/a & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix}a & b\\ 0 & c\end{pmatrix}\begin{pmatrix}a' & 0\\ 0 & 0\end{pmatrix}+\begin{pmatrix}0 & b'\\ 0 & c'\end{pmatrix}\begin{pmatrix}a & b\\ 0 & c\end{pmatrix}\begin{pmatrix}0 & 0\\ 0 & 1/c\end{pmatrix}\in A$$

が成り立ち，$R=A$となる.

24. mに関する帰納法で$A^m+B=R$を示す．$m=1$のときはよい．$m>1$とし$A^{m-1}+B=R$を仮定する．$a+b=1$ $(a\in A^{m-1}, b\in B)$とする． $1=1^2=(a+b)^2=a^2+ab+ba+b^2$．$a^2\in A^{2(m-1)}\subseteqq A^m$であり，$a+b=1$からは$ba+b^2=b$．したがって，$1\in A^m+B$.

28. $f\colon \boldsymbol{Q}\to\boldsymbol{Q}$を環準同型，$\dfrac{n}{m}\in\boldsymbol{Q}$とする．$f(n)=f\left(m\cdot\dfrac{n}{m}\right)=f(m)\cdot f\left(\dfrac{n}{m}\right)$. $f(m)=f(m\cdot 1)=m\cdot f(1)=m$．したがって，$n=m\cdot f\left(\dfrac{n}{m}\right), f\left(\dfrac{n}{m}\right)=\dfrac{n}{m}$.

29. $f\colon \boldsymbol{Q}\to\boldsymbol{Q}$を加法群$\boldsymbol{Q}$の自己準同型，$\dfrac{n}{m}\in\boldsymbol{Q}$とする．$f\left(\dfrac{n}{m}\right)=\dfrac{n}{m}\cdot f(1)$が成り立つから$\mathrm{End}(\boldsymbol{Q})\to\boldsymbol{Q}$を$f\to f(1)$ときめたらよい． $f\colon \boldsymbol{Z}/(m)\to\boldsymbol{Z}/(m)$が加法群$\boldsymbol{Z}/(m)$の自己準同型，$\bar{a}=a+(m)\in\boldsymbol{Z}/(m)$ならば$f(\bar{a})=a\cdot f(\bar{1})$であるから，$\mathrm{End}(\boldsymbol{Z}/(m))\to\boldsymbol{Z}/(m)$を$f\to f(\bar{1})$ときめたらよい.

31. $f\to f(x)$はRから$\boldsymbol{R}$への全射環準同型である.

36. 例えば，$n=2$で$x_1=\alpha(a_1)\alpha(b_1)^{-1}$, $x_2=\alpha(a_2)\alpha(b_2)^{-1}$とかいたとき，$a_1'=a_1b_2$,

$a_2'=a_2b_1$，$b=b_1b_2$ とおけば，$x_1=\alpha(a_1')\alpha(b)^{-1}, x_2=\alpha(a_2')\alpha(b)^{-1}$ とあらわされる．

41.　写像 $K[x]\to K$，$a_nx^n+\cdots+a_1x+a_0\to a_0$ は一意かつ全射環準同型．

44.　A を R のイデアル $(\neq\{0\})$ とする．A は $\dfrac{m}{n}$ で $m>0$ なものを含んでいる．このような m の中で最小なものをえらび，改めて $\dfrac{m}{n}$ とかく．このとき，$\dfrac{m'}{n'}\in A$ ならば $m'=mq+r\ (0\leqq r<m)$ とおけば $\dfrac{r}{n'}=\dfrac{m'}{n'}-\dfrac{m}{n}\cdot\dfrac{nq}{n'}\in A$ であるから $r=0$．したがって，$A=\left(\dfrac{m}{n}\right)$．

46.　$a+b\alpha$ のノルムは a^2-ab+b^2 で与えられる．

48.　$a_1,a_2,\cdots,a_n$ が最小公倍元 l をもてば $(l)=\bigcap_{i=1}^n(a_i)$ であり，逆も正しい．

51.　pu は 0 でも単元でもない．$pu=ab$ とおく．$p=abu^{-1}$ から a が単元か bu^{-1} が単元である．$bu^{-1}=v$ が単元ならば $b=uv$ も単元である．

52.　$ab=pc$ とかく．$a\neq0, b\neq0$ としてよい．$c\neq0$ である．a が単元ならば $b=pca^{-1}$ で $p|b$ である．b が単元のときも同じであるから a も b も単元でないとする．c が単元なら pc は素元 (前問)，$pc=ab$ から a または b が単元となり矛盾．したがって，c も単元でない．$a=p_1^{e_1}\cdots p_n^{e_n}, b=p_1^{f_1}\cdots p_n^{f_n}, c=p_1^{g_1}\cdots p_n^{g_n}\ (e_i,f_i,g_i\geqq0)$ とかける．ここで同じ i に対して e_i,f_i,g_i が同時に 0 になることはないとしてよい．$p_1^{e_1}\cdots p_n^{e_n}p_1^{f_1}\cdots p_n^{f_n}=pp_1^{g_1}\cdots p_n^{g_n}$ から $p\sim p_i$ をみたす i がある．$e_i>0$ ならば $p|a$．$e_i=f_i=0$ ならば $g_i>0$．これは矛盾．したがって，$e_i=0$ ならば $f_i>0$ で $p|b$．

56.　(3)　$\boldsymbol{Z}/(2)[x]$ で $\bar{f}(x)$ が既約であることを示せばよい．もし可約ならば，1 次の因子をもつ．しかし，$\bar{f}(\bar{0})=\bar{f}(\bar{1})=\bar{1}\neq\bar{0}$ でこれは矛盾．

58.　$f=a\cdot f_1, h=\dfrac{c}{b}\cdot h_1\ (a,b,c\in\boldsymbol{Z},\ f_1,h_1$ は原始多項式) とあらわせば，$ab\cdot f_1=c\cdot gh_1$ で，これから $c=\pm ab$．$\dfrac{c}{b}=\pm a$ で $h\in\boldsymbol{Z}[x]$．

59.　$f(x)=x^5+x^4-2x^3+3$ が 1 次因子 $x-a\ (a\in\boldsymbol{Z})$ をもてば $f(a)=0$, $a|3$．これから $a=\pm1$ または ±3 であるが $f(\pm1)\neq0$，$f(\pm3)\neq0$ で矛盾．$f(x)$ は 1 次因子をもたない．$f(x)=(ax^2+bx+c)(dx^3+ex^2+gx+h)$ とおいて $a=b=c=1$，$d=1$，$e=0$，$g=-3, h=3$ をうる．

60.　x^4+1 が $\boldsymbol{Q}$ で可約として $x^4+1=f_1(x)\cdots f_n(x)$ と既約多項式の積に分解する．$\boldsymbol{R}$ では $x^4+1=(x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1)$ と既約多項式の積に分解できる (2.6 節例 12)．$f_i(x)$ はモニックとしてよいから分解の一意性によって $n=2, f_1(x)=x^2+\sqrt{2}x+1, f_2(x)=x^2-\sqrt{2}x+1$ であるが，これは $f_i(x)$ が $\boldsymbol{Q}$ の上の多項式であることに矛盾する．

演習問題 3

1.　$(-a)x+ax=(-a+a)x=o_R\cdot x=o_M$ から $(-a)x=-(ax)$．

4.　$Rx_1+\cdots+Rx_n=\{a_1x_1+\cdots+a_nx_n|\ a_1,\cdots,a_n\in R\}$ は R の元 a と S の元 x に対して ax なる形の M の元の有限和の全体に等しい．また，$Rx_1+\cdots+Rx_n$ が S を含む M の部分加群の中で最小であることを示してもよい．

5.　$a \in R, x \in S$ とする．x はいずれかの M_i に属するが ax も同じ M_i に属するから，ax なる形の M の元の有限和とは $x_1+\cdots+x_n$ ($x_i \in M_i$) の形をしている．また，$M_1+\cdots+M_n$ が S を含む M の部分加群の中で最小であることを示してもよい．

7.　写像 $R/\mathrm{Ann}_R M \times M \to M$, $(a+\mathrm{Ann}_R M, x) \to ax$ が一意写像であることを示せ．

8.　$M'=Rx_1+\cdots+Rx_n$,　$M/M'=R\cdot(y_1+M')+\cdots+R\cdot(y_m+M')$ ならば，$M=Rx_1+\cdots+Rx_n+Ry_1+\cdots+Ry_m$ である．

9.　(2)　$au+p^m v=1$ ($u, v \in \boldsymbol{Z}$) とおくと $\dfrac{b}{p^n}=p^{m-n}\cdot\dfrac{b}{p^m}=p^{m-n}\cdot\dfrac{bau}{p^m}+p^{m-n}\cdot bv$. したがって，$\dfrac{b}{p^n}+\boldsymbol{Z}=p^{m-n}\cdot bu\cdot\dfrac{a}{p^m}+\boldsymbol{Z}\in H$.　(3)　$\boldsymbol{Z}_{p^\infty} \neq H$ から $\dfrac{1}{p^n}+\boldsymbol{Z} \notin H$ なるものがある．(2) から $\dfrac{1}{p}+\boldsymbol{Z}\in H$ であるから $s>1$. $\dfrac{1}{p^s}+\boldsymbol{Z}\in H$ から $s \geqq m$ ならば $\dfrac{a}{p^s}+\boldsymbol{Z} \in H$ は明らか．逆に，H から $\dfrac{a}{p^m}+\boldsymbol{Z}$ をとる．$m>s$ ならば $m \geqq s+1$. (2) から $\dfrac{1}{p^{s+1}}+\boldsymbol{Z}\in H$ となり矛盾．したがって，$m \leqq s$ でなければならない．

13.　(2)　$x, y \in Ra$ ならば $x-y, xy \in Ra$ であるから，Ra が部分環 $\Leftrightarrow$ $Ra \ni 1$ $\Leftrightarrow$ a が R の単元．(3)　$a'a=1$ とおけば写像 $R \to Ra$,　$b \to (ba')a$ は環同型．

14.　R-同型 $R/A \to R/B$ を f とかく．$f(1+A)=a+B$,　$f^{-1}(1+B)=b+A$ とおく．$ba-1 \in B$ である．A の任意の元 c に対して，$ca+B=f(c+A)=\bar{0}$,　$ca \in B$ であるから $c=(ba-1)c-b(ac)$ は B に属する．

19.　$f: M \to M$ が 0 でない R-準同型ならば，$f(M)=M, \mathrm{Ker}\, f=\{0\}$ で f は R-同型．

21.　(1)　$x, y \in M$ に対して $\beta(x)=\beta(y)$ を仮定する．$\gamma g(x)=g'\beta(x)=g'\beta(y)=\gamma g(y)$ から $g(x)=g(y), x-y \in \mathrm{Ker}\, g=f(L)$. したがって，$x-y=f(z)$ をみたす $z \in L$ がある．$f'\alpha(z)=\beta f(z)=\beta(x-y)=0$ から $\alpha(z)=0$ で $z=0$.　$x-y=f(z)=0$ で $x=y$ をうる．

22.　$\boldsymbol{Z}/(4) \xrightarrow{\alpha} \boldsymbol{Z}/(4) \xrightarrow{\beta} \boldsymbol{Z}/(4)$ とし $\alpha(a+(4))=2a+(4), \beta(b+(4))=2b+(4)$ ときめたらよい．

23.　(1)　$x+y \neq x, y$ から $x+y=0$ とする．$x=-y=y$ で矛盾．したがって，$x+y=z$.　(2)　$x, y, z, 0 \in \boldsymbol{Z}x+\boldsymbol{Z}y$ であるから $M=\boldsymbol{Z}x+\boldsymbol{Z}y$.　$x \in \boldsymbol{Z}x \cap \boldsymbol{Z}y$ ならば，$x=ay$ とかける．$a \neq 1$.　$a<0$ ならば $x=-x=-(ay)=(-a)y$. したがって，$a>0$ としてよい．$a=2q+r$ とかく．$x=ay=2qy+ry=ry=0$ または y. いずれにしても矛盾．同じように y, z を含まないから $\boldsymbol{Z}x \cap \boldsymbol{Z}y=\{0\}$.

29.　M' の元 x を $x=x_1+x_2$ ($x_i \in M_i$) とかく．$x-x_1=x_2 \in M' \cap M_2$ であるから $x=x_1+x_2 \in M_1+(M_2 \cap M')$. したがって，$M'=M_1+(M_2 \cap M')$.　$M_1 \cap (M_2 \cap M') \subseteqq M_1 \cap M_2=\{0\}$ から $M'=M_1 \oplus (M_2 \cap M')$.

34.　$\Rightarrow$: 補題 3.5 から $M=N \oplus f(M/N)$. このとき $p: M \to N$ を 1-射影ときめる．N の任意の元 y に対して $p\nu(y)=p(y)=y$ から $p\nu=1_N$.　$\Leftarrow$: 補題 3.5 から $M=\mathrm{Ker}\, p \oplus N$. このとき 1-射影を $p_1: M \to \mathrm{Ker}\, p$ とかき $f: M/N \to M$ を $f(x+N)=p_1(x)$ ときめる．$\pi f(x+N)=\pi(p_1(x))=p_1(x)+N=x+N$ で $\pi f=1_{M/N}$.

37.　$\boldsymbol{Q}$ が 1 元からなる基底をもったとする．$\boldsymbol{Q}=\boldsymbol{Z}\cdot\dfrac{b}{a}$,　$(a, b)=1$ とする．ある $n \in \boldsymbol{Z}$ があって $n\cdot\dfrac{b}{a}=1$,　$a=nb$. これは $(a, b)=1$ に矛盾する．$\boldsymbol{Q}$ が 2 個以上の元からなる基

底をもったとする．$\boldsymbol{Q}=\boldsymbol{Z}\cdot\frac{b}{a}+\boldsymbol{Z}\cdot\frac{b'}{a'}+\cdots$, $(a,b)=(a',b')=\cdots=1$ とする．$\frac{b}{a}\neq 0$, $\frac{b'}{a'}\neq 0$ から $ab'\neq 0$, $a'b\neq 0$. その上 $ab'\cdot\frac{b}{a}+(-a'b)\cdot\frac{b'}{a'}=0$ でこれに矛盾．

39.　⇒: 定理 3.6, 3.7 による．⇐: R-加群 N, N の元 $y_1, y_2, \cdots, y_n$ に対して写像 f を $f(x_i)=y_i$ ときめる．仮定から R-準同型 g があって $g(x_i)=y_i$. このような g の一意性は (1) から分かる．定理 3.7 が適用できる．

40.　M の基底を (x_i) とし，$f(x_i)=g(y_i)$ となる $y_i\in L$ をとる．このとき $h: M\to L$, $a_1x_1+\cdots+a_nx_n\to a_1y_1+\cdots+a_ny_n$ ときめる．

41.　⇒は明らか．⇐: M の基底を $x_1, x_2, \cdots, x_n$, N の基底を $y_1, y_2, \cdots, y_n$ とし，$f: M\to N$ を $f(x_i)=y_i$ ときめる．f は全単射である．

43.　$AB\subseteqq A, B$ から $AB\subseteqq A\cap B$. 逆に，$A\cap B\ni a=b$ をとる．$1=a'+b'$ $(a'\in A, b'\in B)$ とかけば $a=aa'+ab'=ba'+ab'\in AB$.　$A+B=B+C=C+A=R$ とする．まず，$A+C=B+C=R$ から $R=R^2=(A+C)\cdot(B+C)\subseteqq AB+C\subseteqq R$. したがって，$AB+C=R$. これから $(AB)C=AB\cap C=A\cap B\cap C$.

46.　$f\in\boldsymbol{Q}^*$ とする．素数 p に対して $p\cdot f\left(\frac{1}{p}\right)=f(1)$. 任意の p が $f(1)$ を割り切るから $f(1)=0$.　$\boldsymbol{Q}$ の元 $\frac{b}{a}$ に対して $a\cdot f\left(\frac{b}{a}\right)=f(b)=b\cdot f(1)=0$.　$a\neq 0$ から $f\left(\frac{b}{a}\right)=0$.

47.　$n=2$ のとき明らかで，$n>2$ とする．$R=A_n+A_1\cap\cdots\cap A_{n-1}$ の証明は，$R=A_n+A_i$ $(i\neq n)$ にしたがって $1=a_{ni}+a_i$ とかき，$1=(a_{n1}+a_1)\cdots(a_{n,n-1}+a_{n-1})=b_n+a_1a_2\cdots a_{n-1}$ をみたす $a_n\in A_n$ があるから，$1\in A_n+A_1\cap\cdots\cap A_{n-1}$ が分かる．次に $A_1, \cdots, A_{n-1}$ に対して $R=A_i+\bigcap_{j\neq i}A_j$ を仮定し，$1=a_i+b_i$ とおく．$A_1, A_2, \cdots, A_n$ に対して $R=A_i+(\bigcap_{j\neq i}A_j)\cap A_n$ を示せばよい．$R=A_i+A_n$ から $1=a_i'+b_i'$ とかく．$1=(a_i+b_i)(a_i'+b_i')=a_i''+b_ib_i'$ をみたす $a_i''\in A_i$ がある．$1\in A_i+(\bigcap_{j\neq i}A_j)\cap A_n$ が分かる．

48.　⇒: $M=N\oplus N'$ ならば，$M/N\cong N'$ から明らか．⇐: M の基底 $x_1, x_2, \cdots, x_m$ と N の基底 $a_1x_1, a_2x_2, \cdots, a_nx_n$ をとる（定理 3.11）．このとき $M/N\cong(\oplus_{i=1}^n R/Ra_i)\oplus R^{m-n}$. 仮定から $\oplus_{i=1}^n R/Ra_i=\{0\}$. 特に各 i に対して $R=Ra_i$. したがって，$N=Ra_1x_1\oplus\cdots\oplus Ra_nx_n=Rx_1\oplus\cdots\oplus Rx_n$.　$M=Rx_1\oplus\cdots\oplus Rx_m=N\oplus(Rx_{n+1}\oplus\cdots\oplus Rx_m)$.

52.　$\boldsymbol{Z}$-加群とみて $\boldsymbol{Z}$ はトーション・フリー加群，$\boldsymbol{Z}/(n)$ はトーション加群．

56.　M が有限生成トーション・フリー加群ならば，$M\cong(\oplus_{i=1}^n R/Ra_i)\oplus R^s$ ではじめの項がきえて R^s のみ残る．逆は明らか．

57.　$32=2^5$ から $(2,2,2,2,2)$ 型，$(2,2,2,2^2)$ 型，$(2,2^2,2^2)$ 型，$(2,2,2^3)$ 型，$(2,2^4)$ 型，$(2^2,2^3)$ 型，(2^5) 型がある．

58.　$\boldsymbol{Z}/(4)\oplus\boldsymbol{Z}/(24)$, $\boldsymbol{Z}/(2)\oplus\boldsymbol{Z}/(50)\oplus\boldsymbol{Z}/(100)$.

59.　$G\cong\oplus_{i=1}^n\boldsymbol{Z}/(p_i^{e_i})$ とおく．$pG=0$ から $p\cdot\boldsymbol{Z}/(p_i^{e_i})=0$ $(1\leqq i\leqq n)$. したがって，$p_i^{e_i}\cdot a=p$ をみたす整数 a が存在するが，素因数分解の一意性から $p_i=p$, $e_i=1$ $(1\leqq i\leqq n)$.

60.　$G\cong^f\oplus_{i=1}^n\boldsymbol{Z}/(p_i^{e_i})$ とかけば $|G|=p_1^{e_1}\cdots p_n^{e_n}$.　$m\,|\,|G|$ ならば $m=p_1^{f_1}\cdots p_n^{f_n}$ $(0\leqq f_i\leqq e_i)$ とかける．このとき $H_i=(p_i^{e_i+f_i})/(p_i^{e_i})$ は $\boldsymbol{Z}/(p_i^{e_i})$ の位数 $p_i^{f_i}$ の部分加群

で，$f^{-1}(H_1 \oplus \cdots \oplus H_n)$ が求めるもの．

演習問題 4

1. (1) は明らか．(2) $k(S_1 \cup S_2)$ は k と K の中間体で $S_1 \cup S_2$ を含む，特に S_1 を含むから $k(S_1) \subseteqq k(S_1 \cup S_2)$．$k(S_1)(S_2)$ は $k(S_1)$ と K の中間体で S_2 を含むから $k(S_1)(S_2) \subseteqq k(S_1 \cup S_2)$．

2. 補題 2.3 を利用．

3. $k=\{0,1,2,\cdots,p-1\}$ のとき 1 と $p-1$ が求めるもの．

4. $p(x)$ が定数ならば $\mathrm{Ker}\, h = k[x]$．$g(x)=x$ にとれば $\alpha=0$，$g(x)=x-1$ にとれば $\alpha=1$．これは矛盾．

6. $\Leftarrow$: $f(x)$ は最小多項式と定数のちがいしかない．

8. $\alpha=\sqrt{2}+\sqrt{3}$ とおく．$2\sqrt{2}=\alpha^2-9\alpha$ から $\sqrt{2} \in \boldsymbol{Q}(\alpha)$．$\sqrt{3}=\alpha-\sqrt{2} \in \boldsymbol{Q}(\alpha)$．$\alpha^2=5+2\sqrt{6}$ から $(\alpha^2-2)^2=24$．α は x^4-10x^2+1 の根．

9. $\boldsymbol{Q}(\sqrt{3}, \sqrt{7})=\boldsymbol{Q}(\sqrt{3}+\sqrt{7})$, $\boldsymbol{Q}(\sqrt{3}, i)=\boldsymbol{Q}(\sqrt{3}+i)$．次数は共に 4．

10. $x^2-2ax+(a^2+b^2)$．

11. $x^4-4x^3-4x^2+16x-8$．

12. x^2+2，x^6+4．

16. $\dfrac{1}{23}(\alpha^3-5\alpha^2+\alpha+15)$．

17. $\alpha=\sqrt{2}+i$ とおけば $1, \alpha, \alpha^2, \alpha^3$．

19. $[K:k]=p>1$ から k に属さない K の元 α がある．$[k(\alpha):k]=p$ で $[K:k(\alpha)]=1$．

20. α が K に属する根ならば $[k(\alpha):k]$ は $[K:k]$ の約数，したがって，1．

24. 逆が正しければ，代数拡大は有限拡大．

27. K が k の代数拡大とする．$k \subseteqq K' \subseteqq K, K'$ が部分環ならば，$K' \ni \alpha \neq 0$ に対し $k(\alpha) = k[\alpha] \subseteqq K'$．これから $\alpha^{-1} \in K'$．逆に，k を含む K の部分環が体ならば，$K \ni \alpha \neq 0$ に対し $k[\alpha]$ は体，$\alpha^{-1} \in k[\alpha]$．ある $f(x) \in k[x]$ があって $f(\alpha)=\alpha^{-1}$．α は $xf(x)-1$ の根となる．

28. n に関する帰納法．$n=1$ のとき $K=k$．$n>1$ とし $\alpha \in K$ が $f(x)$ の根ならば，$k(\alpha)$ で $f(x)=(x-\alpha)f_1(x)$ と分解される．$f_1(x)$ の根はすべて K にあるから K は $f_1(x)$ の $k(\alpha)$ 上の分解体．$[k(\alpha):k] \leqq n, [K:k(\alpha)] \leqq (n-1)!$ から $[K:k] \leqq n!$．

29. $\alpha=\dfrac{1+i}{\sqrt{2}}$ とおけば x^4+1 の 4 つの根は $\pm\alpha, \pm\alpha^3$．$\boldsymbol{Q}(\alpha)$ が分解体，その次数は 4．

30. $f(x)=x^p-1=(x-1)(x^{p-1}+\cdots+x+1)$．$g(x)=x^{p-1}+\cdots+x+1$ は $\boldsymbol{Q}$ 上既約 (2.6 節例 15)．$g(x)$ の 1 つの根を α とおけば $\alpha^2, \cdots, \alpha^{p-1}$ も $g(x)$ の根．したがって，$\boldsymbol{Q}(\alpha)$ は $g(x)$ の分解体で，$f(x)$ の分解体でもある．次数は $p-1$．

31. $f(x)$ は k 上既約 (演習問題 4 の 40) で，$k[x]/(f(x))$ に根 α をもつ．このとき $f(x)=(x-\alpha)(x-\alpha^2)(x-\alpha^4)$．

32. K は $f(x)=x^{p^n}-x$ の根の全体と一致し，K において $f(x)=\prod_{\alpha \in K}(x-\alpha)$ と分解される．$K=\{0, \alpha_1, \cdots, \alpha_{p^n-1}\}$ とかけば，　$f(x)=x^{p^n}-(\alpha_1+\cdots+\alpha_{p^n-1})x^{p^n-1}+\cdots+(-1)^{p^n-1}\alpha_1\cdots\alpha_{p^n-1}x$．これから $\alpha_1+\cdots+\alpha_{p^n-1}=0, (-1)^{p^n-1}\alpha_1\cdots\alpha_{p^n-1}=-1$．$p=2$

のときは $\alpha_1\cdots\alpha_{p^n-1}=1=-1$，$p>2$ のときは $\alpha_1\cdots\alpha_{p^n-1}=-1$.

33.　$f(x)$ は最小多項式と定数のちがいしかない.

34.　特性多項式は重根をもたない (定理 4.18 の証明).

35.　$m|n$ とし $f(x)$ を k 上の m 次モニックな既約多項式とする．位数 p^m の K の部分体 K' がただ 1 つ存在する．$f(x)$ は K' の特性多項式 $x^{p^m}-x$ を割り切る．$(x^{p^m}-x)|(x^{p^n}-x)$ から $f(x)|(x^{p^n}-x)$．次に，$x^{p^n}-x$ を割り切るものはこれ以外にないことを示す．k 上 s 次の既約多項式 $g(x)$ が $g(x)|(x^{p^n}-x)$ ならば，$g(x)$ の根 α は $x^{p^n}-x$ の根で，$\alpha\in K$．その上 $|k(\alpha)|=p^s$ から $s|n$ (定理 4.19).

36.　$x^4-x=x(x+1)(x^2+x+1)$，$x^8-x=x(x+1)(x^3+x+1)(x^3+x^2+1)$.

39.　$2^{10}=1024\equiv 1 \pmod{11}$.

43.　$1+\alpha$.

45.　$2\alpha^2+\alpha+1$.

49.　G を K^* の位数 n の部分群とする．G には最大位数 N の元があり，G の元の位数はすべて N の約数である (3.6 節例 6)．G の任意の元 α は $\alpha^N=1$ をみたすから $n\leqq N$ (定理 2.15) であり，また，$N|n$ から $N=n$．G は位数 n の元をもつ.

50.　K^* の生成元を α とかけば $K=\{0,1,\alpha,\alpha^2,\cdots\}$．任意の自然数 m に対して $\alpha^m\cdot\alpha^n=1$ をみたす自然数 n がある．したがって，$\alpha^i=1$ となる最小の自然数があり，これを改めて m とかけば $K=\{0,1,\alpha,\cdots,\alpha^{m-1}\}$.

参考文献

この本を書くのに参考にした本，更に進んで勉強するときの本等をあげておこう．

[1] 浅野啓三，永尾汎：『群論』(岩波書店，1965年)

[2] 彌永昌吉，小平邦彦：『現代数学概説Ⅰ』(岩波書店，1961年)

[3] 高橋磐郎：『組合せ理論とその応用』(岩波書店，1979年)

[4] 永尾汎：『群論の基礎』(朝倉書店，1967年)

[5] 服部昭：『現代代数学』(朝倉書店，1968年)

[6] 松坂和夫：『代数系入門』(岩波書店，1978年)

[7] 松坂和夫：『集合・位相入門』(岩波書店，1983年)

[8] 守屋美賀雄：『代数学 上，下』(朝倉書店：上1949年，下1950年)

[9] F.W. Anderson and K.R. Fuller: *Rings and Categories of Modules* (Springer-Verlag, 1973年)

[10] D.M. Burton: *A First Course in Rings and Ideals* (Addison-Wesley, 1970年)

[11] B. Hartley and T.O. Hawkes: *Rings, Modules and Linear Algebras* (Chapman and Hall, 1976年)

[12] T. Head: *Modules, A Primer of Structure Theorems* (Brooks/Cole, 1974年)

[13] R. Lidl and H. Niederreiter: *Introduction of finite fields and their applications* (Cambridge Univ. Press, 1986年)

索　　引

あ　行

アイゼンシュタインの規準　103
アーベル群　3
　——の基本定理　150
R-自己準同型　124
　——環　124
R-準同型　120
　——写像　120
　自然な——　121
　標準的——　121
　誘導された——　122
R-同型　120
R-左加群　112
位数
　群の——　4
　元の——　28
一意分解整域　95
1次独立　129
一般線型群　5
イデアル　61
　自明な——　61
因数定理　86
運動　7
n 次の対称群　6
m 重根　182
演算　1
円周等分多項式　105
オイラーの関数　37
オイラーの定理　39

か　行

階数　134, 145
外部直和　127
ガウスの整数環　60
ガウスの補題　100
下界　14
可換環　56
可換群　3
可換図型　122
核　27, 67
拡大次数　169
拡大体　159
加法　55
　——群　2
可約多項式　93
ガロア体　183
環　55
　——の準同型定理　69
　——の直積　106
環準同型　67
　——写像　67
　自然な——　69
　標準的——　69
完全　154
完全代表系　17
環同型　67
簡約律　5
奇置換　45
基底　129
逆元　3, 58
既約剰余類　38
既約多項式　93
共役　31
　——部分群　51
　——類　31
行列環　56
極大イデアル　74
極大部分加群　117
偶置換　45
クラインの4元群　32
群　1
　——の準同型定理　27
係数環　81
結合法則　2
原始 m 乗根　38

原始既約多項式　187
原始元　186
原始多項式　100
交換子　22
　——群　22
交換法則　3
合成数　15
交代群　46
合同　19
恒等写像　120
公倍数　36
公約数　34
互換　41
根　83

さ 行

最高次係数　81
最小公倍元　91
最小公倍数　36
最小多項式　163
最大公約元　91
最大公約数　34
差積　44
サルスの法則　48
三角行列環　60
4 元群　32
4 元数環　59
自己準同型　57
　——環　57
自己同型　50
指数　19
　——法則　9
次数　81, 163, 169
自然な R-準同型　121
自然な環準同型　69
自然な準同型　26
実数体　59
自明なイデアル　61
自明な部分加群　114
自明な部分群　11
自明な分解　92
射影　126, 128
斜体　59
シュアーの補題　154
自由加群　129
重根　182
巡回加群　117
巡回群　31
巡回置換　41
巡回部分加群　115
　生成された——　115
巡回部分群　13
　生成された——　13
準同型　24
　——写像　24
　——定理　27, 69, 122
　自然な——　26
　標準的——　26
商　15, 84
上界　14
乗積表　6
商体　78
乗法　55
　——群　2
剰余　15, 84
　——加群　118
　——環　65
　——群　23
　——類　19
除法の定理　15, 84
整域　58
正規化群　50
正規部分群　21
制限写像　121
整数環　56
整数論の基本定理　90
生成系　13
生成元　13, 31, 116
生成された巡回部分加群　115
生成された巡回部分群　115
生成された左イデアル　62
生成された部分加群　116
生成された部分群　13
正則　5, 59
積
　元の——　2, 55, 64
　部分集合の——　18
全射環準同型　67
全射準同型　24
素イデアル　95

像 27, 67
双対加群 136
素元 92
素数 15
素体 75

た 行

体 59
第一同型定理 51
対称群 6
代数拡大 171
代数学の基本定理 87
代数的 161
——拡大体 171
——数 163
——に閉じている 173
——閉体 87, 173
——閉包 173
第二同型定理 51
代入 83
代表元 17
互いに素 35
多項式 79
——環 81
単位群 6
単位元 2, 56
単因子 150
単元 58
単項イデアル 62
——整域 62
単項左イデアル 62
単項右イデアル 62
単根 182
単射準同型 24
単射環準同型 67
単純拡大 161
単純加群 115
単純環 63
単純群 21
置換 6
中間体 159
中心 31
超越数 163
超越的 161
重複度 150
直既約 144
直積
——に分解される 53
環の—— 106
群の—— 53
直和
——因子 125
——に分解される 125
——分解 125
定数多項式 81
転位 45
添加した体 159
同型 24
——写像 24
同伴 90
特殊線型群 5
特性多項式 183
トーションの加群 146
トーション元 145
トーション部分加群 145
トーション・フリー加群 146
トーラス群 12

な 行

内部自己同型 26
内部直和 124
二項定理 103, 191
二面体群 8, 49
入射 126, 128
ノルム 85

は 行

倍元 90
倍数 15
p 群 31
左イデアル 61
——の和 62
生成された—— 62
左加群 112
左剰余類 16
左合同 16
左ベクトル空間 113
左零化イデアル 123
左零因子 58
微分 183, 191

標準的 R-準同型　121
標準的環準同型　69
標準的準同型　26
標数　71
フェルマーの定理　39
複素数体　59
符号　46
不定元　81
部分加群　114
　自明な——　114
　生成された——　116
部分環　60
部分群　10
　自明な——　11
　生成された——　13
部分体　60
不変因子　145, 150
分解体　175
分配法則　56
べき零元　108
包含写像　121

ま　行

右イデアル　61
右逆元　4
右合同　18
右剰余類　19
右単位元　4
右ベクトル空間　113
右零因子　58
無限群　4
モジュラー変換群　49
モニックな多項式　81

や　行

約元　90
約数　15
有限拡大　169
有限群　4
有限次拡大体　169
有限生成加群　116
　——の構造定理　140
有限体　179
誘導された R-準同型　122
有理関数体　83, 160
有理式　160
有理数体　59
ユークリッド整域　85

ら　行

ラグランジュ　20
類等式　31
類別　17
零因子　58
零加群　114
零環　58
零元　3, 56
零写像　120
零多項式　81

わ　行

和
　元の——　2, 55
　左イデアルの——　62
　部分加群の——　115

著者略歴

倉田 吉喜 (くらた よしき)

1953年 北海道大学理学部数学科卒業

1955年 北海道大学大学院理学研究科修士課程修了

1956年 北海道大学理学部助手

1962年 山口大学文理学部講師

1964年 山口大学文理学部助教授

1966年 山口大学文理学部教授

1978年 山口大学理学部教授,
現在に至る(理学博士).

現代数学ゼミナール 16

代 数 学

© 1992 倉田吉喜 Printed in Japan

1992年4月10日 初 版 発 行

著 者 倉 田 吉 喜

発行者 櫻 井 慧 子

発行所 株式会社 近代科学社

〒162 東京都新宿区市ケ谷田町2-7-15
電話 03(3260)6161 振替(東京)6-7625

定価 2800 円

エイトシステム・大日本法令印刷 ISBN4-7649-1029-2